FortiClient EMS Study Guide

for FortiClient EMS 6.2

Fortinet Training

http://www.fortinet.com/training

Fortinet Document Library

http://docs.fortinet.com

Fortinet Knowledge Base

http://kb.fortinet.com

Fortinet Forums

https://forum.fortinet.com

Fortinet Support

https://support.fortinet.com

FortiGuard Labs

http://www.fortiguard.com

Fortinet Network Security Expert Program (NSE)

https://www.fortinet.com/support-and-training/training/network-security-expert-program.html

Feedback

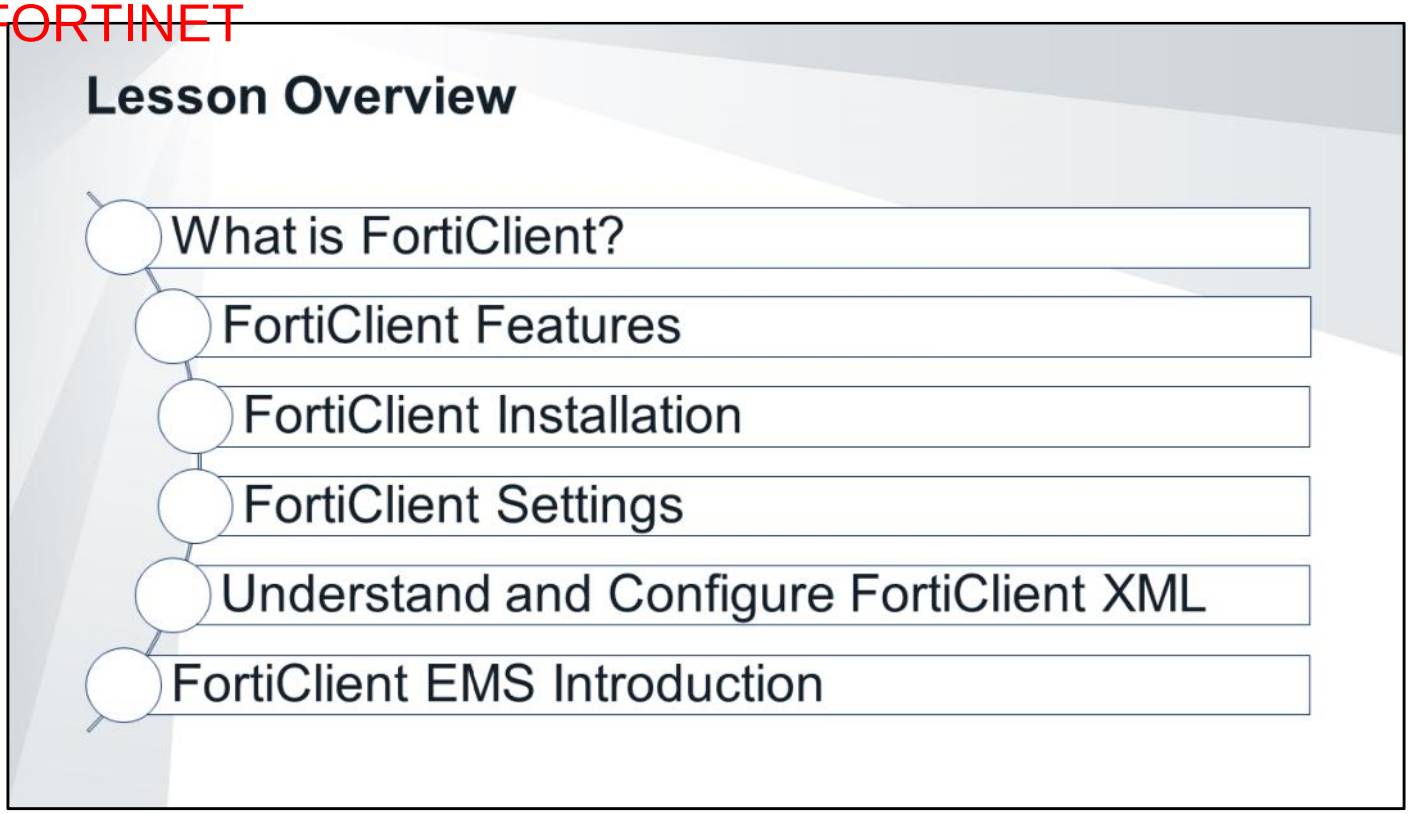
Email: courseware@fortinet.com

12/17/2019

TABLE OF CONTENTS

01 Introduction to FortiClient and FortiClient EMS 4
02 FortiClient Enterprise Management System (EMS) 84
03 FortiClient Deployment and Provisioning Using FortiClient EMS 147
04 Diagnostics and Troubleshooting 206

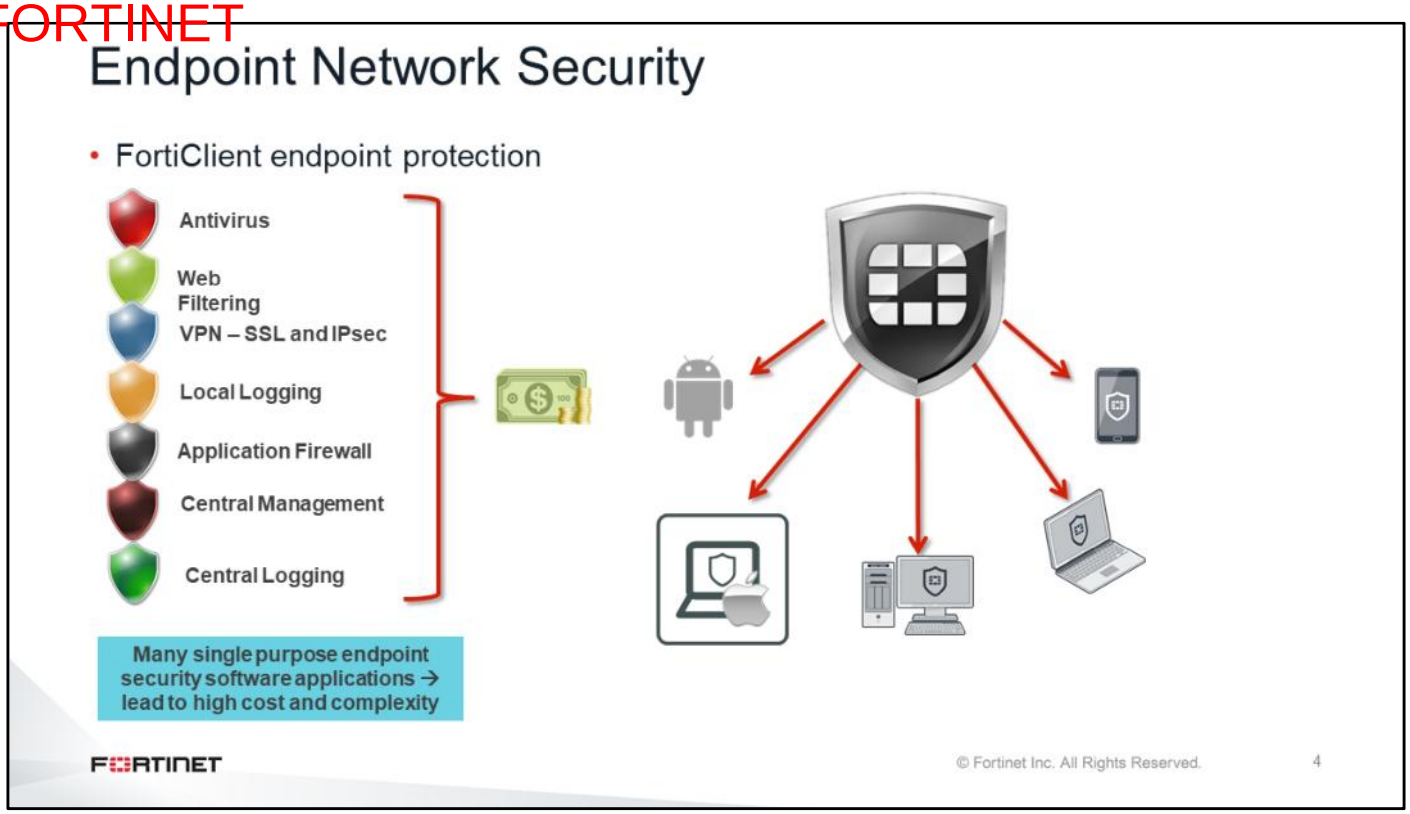
In this lesson, you will learn how to integrate FortiClient into your existing network, and manage the security of multiple endpoint devices from a single management console, such as FortiClient Enterprise Management Server (EMS).



In this lesson, you will learn about the topics shown on this slide.

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating an understanding of what FortiClient is and what it does, you will be able to understand how FortiClient fits in to your network.

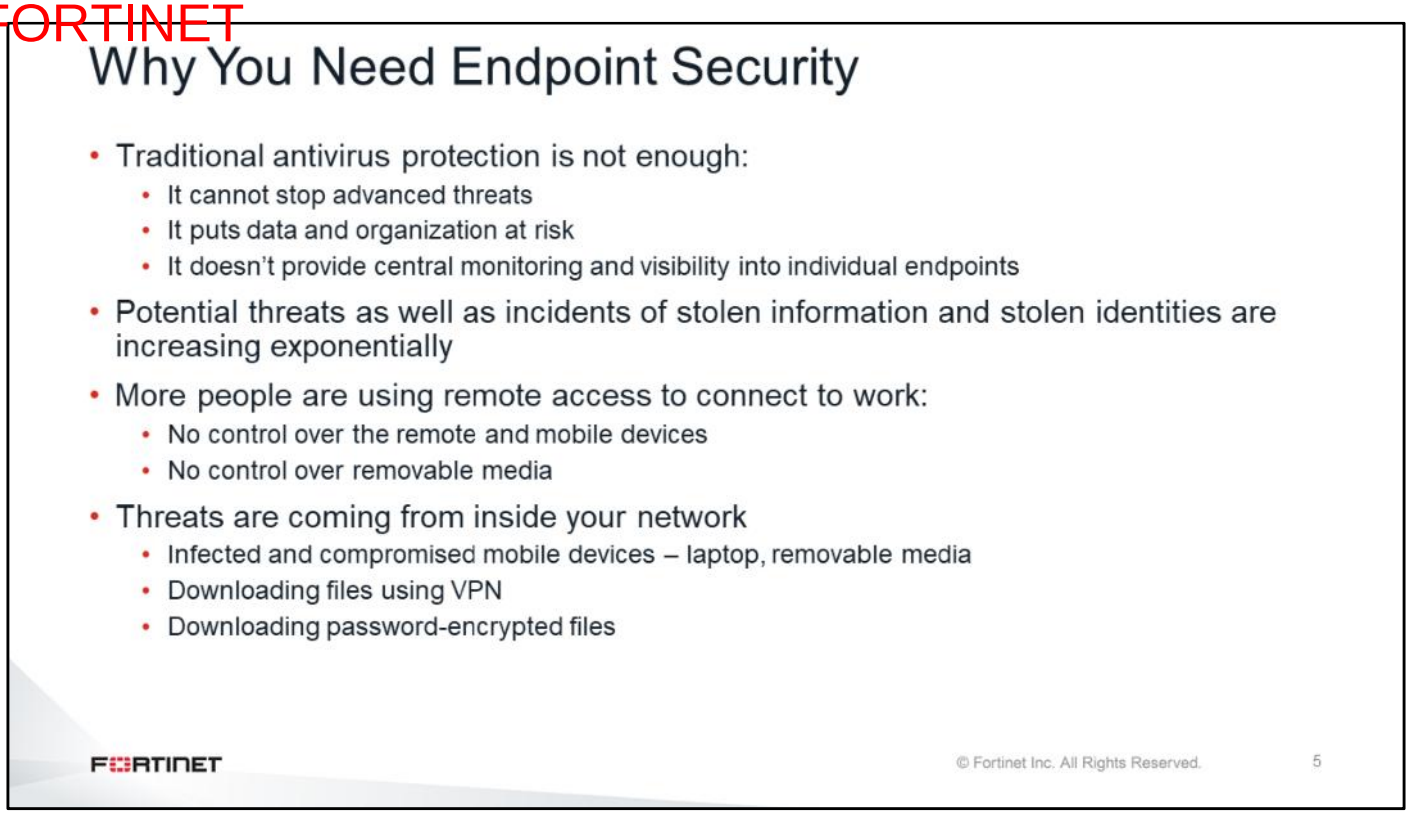


In a typical endpoint network security solution, multiple instances of single-purpose software applications are used. Each application provides a specific service, including antivirus protection, web filtering, VPN access, application firewall, and so on.

Many endpoint security solutions are not capable of providing central management, central logging, and other features.

When several different applications are used, most times they all are made by different vendors. Using applications from multiple vendors can introduce unwanted complexity, create many potential points of failure, and increase the cost of initial installation and ongoing operation.

On the other hand, FortiClient offers comprehensive endpoint protection for your Windows-based and Mac-based desktops, laptops, file servers, and mobile devices. FortiClient can safeguard your systems with advanced security technologies and provide a single management console.



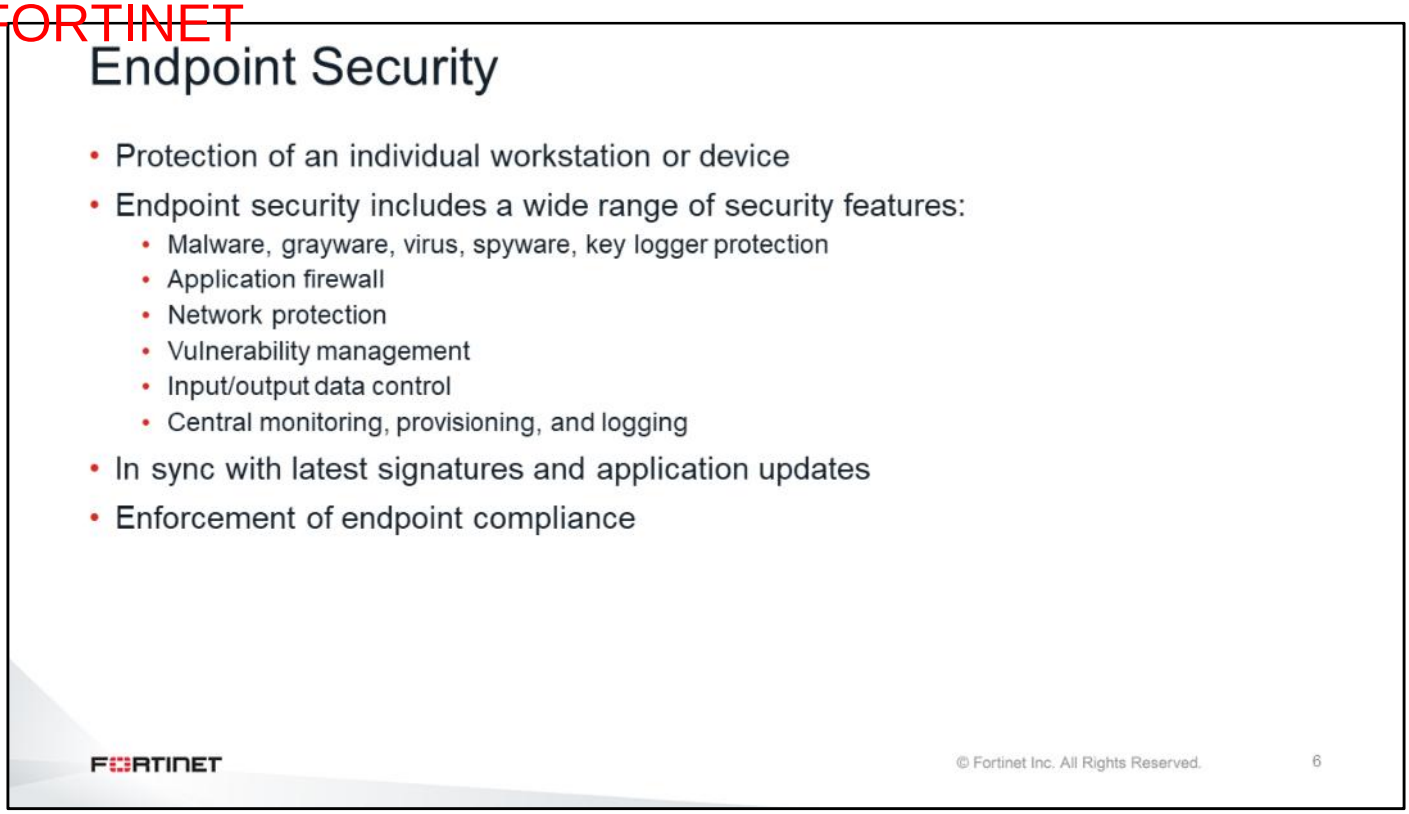
Traditional antivirus software can protect your endpoints from known viruses, but may be unable to detect and protect against advanced threats. This can result in data being lost or compromised.

Present day attackers use advanced methods to hijack your identity, such as social media accounts, and access your banking information. Sometimes, this information is browser or application-based, and antivirus software can do a little to protect it.

More and more people connect to corporate networks from Wi-Fi hotspots, providing no control over remote or mobile devices.

Not only do threats come from outside your network, people often bring mobile devices inside your network, which may be compromised. They also use your VPN to download files, which may be contain potential issues.

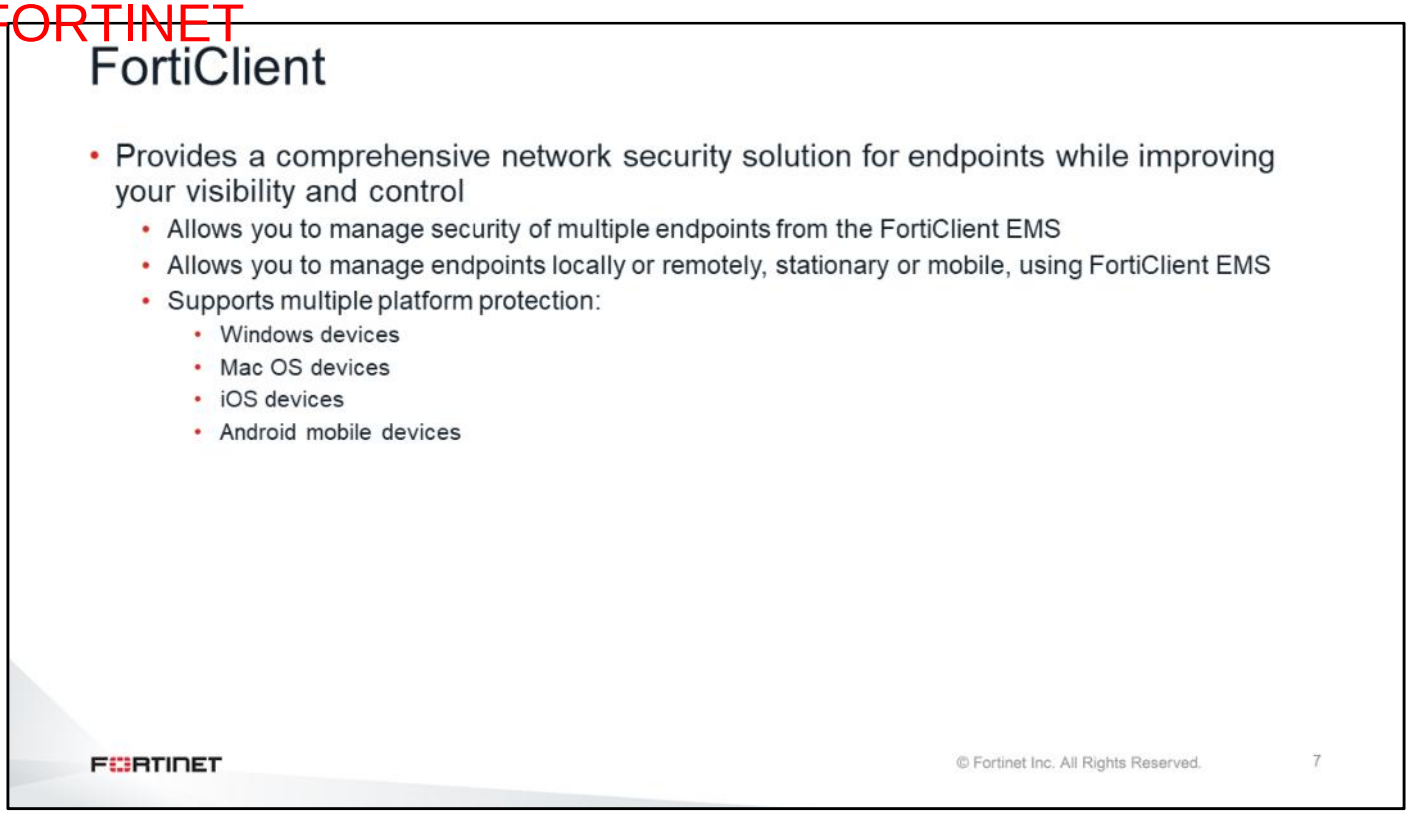
This is why you need endpoint security!



Standard security software can provide basic protection, but endpoint security provides basic security plus much more.

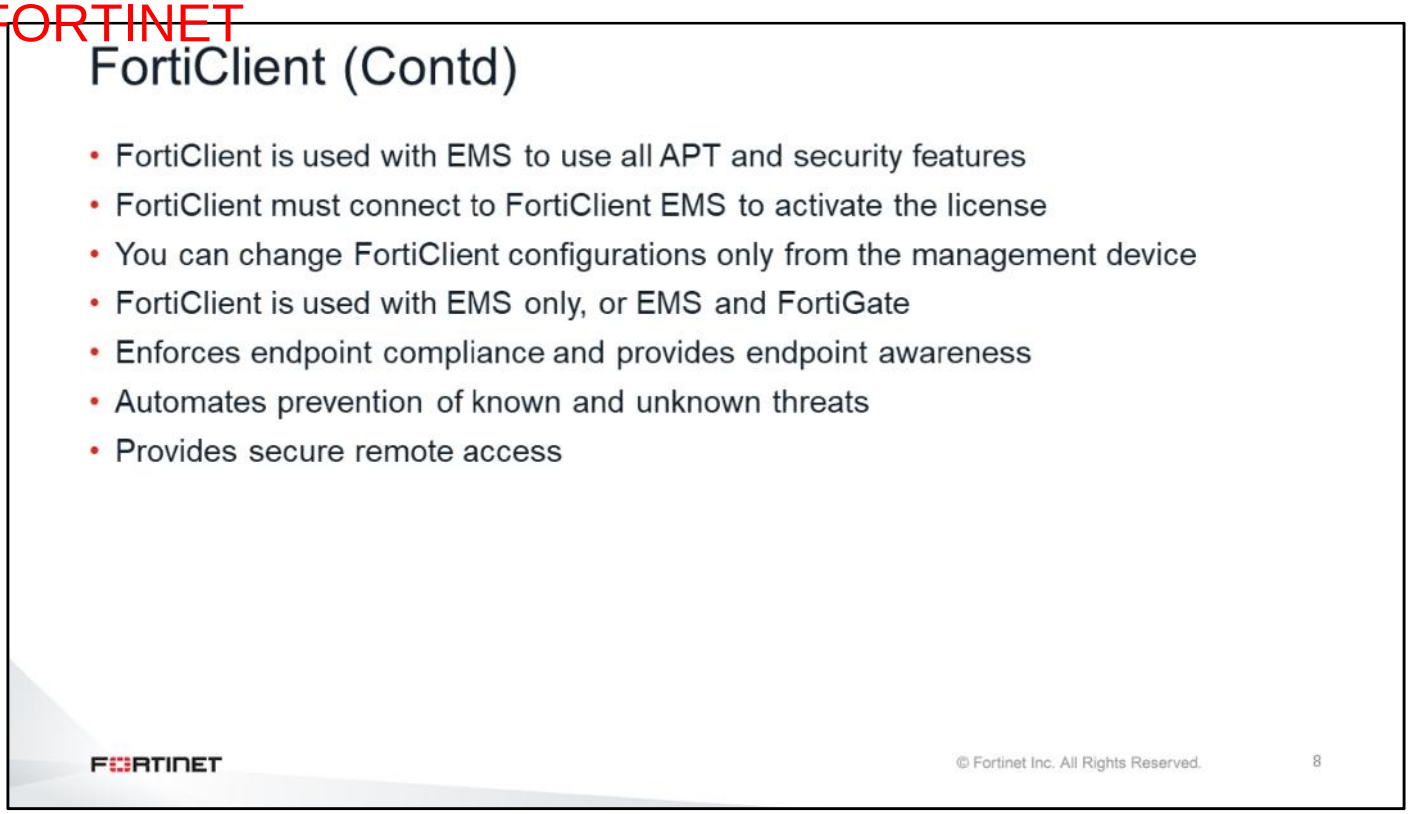
Endpoint security provides an antivirus program and much more to protect your devices and it creates a barrier between your network and the outside. Endpoint security provides antivirus updates, antimalware, IPS/IDS signatures, and updates.

Endpoint security also forces endpoint compliance, which requires endpoints devices to comply with specific criteria before they can gain access to the network.



FortiClient provides comprehensive endpoint protection for your Windows-based and Mac-based desktops, laptops, file servers, and mobile devices. It helps you to safeguard your systems with advanced security technologies, all of which you can manage from a single management console.

FortiClient enables every device—local or remote, stationary or mobile—to integrate with your FortiGate and FortiClient EMS. FortiClient supports Windows, Mac OS, iOS, and Android mobile devices, and also integrates your home offices, mobile workers, and visiting partners.



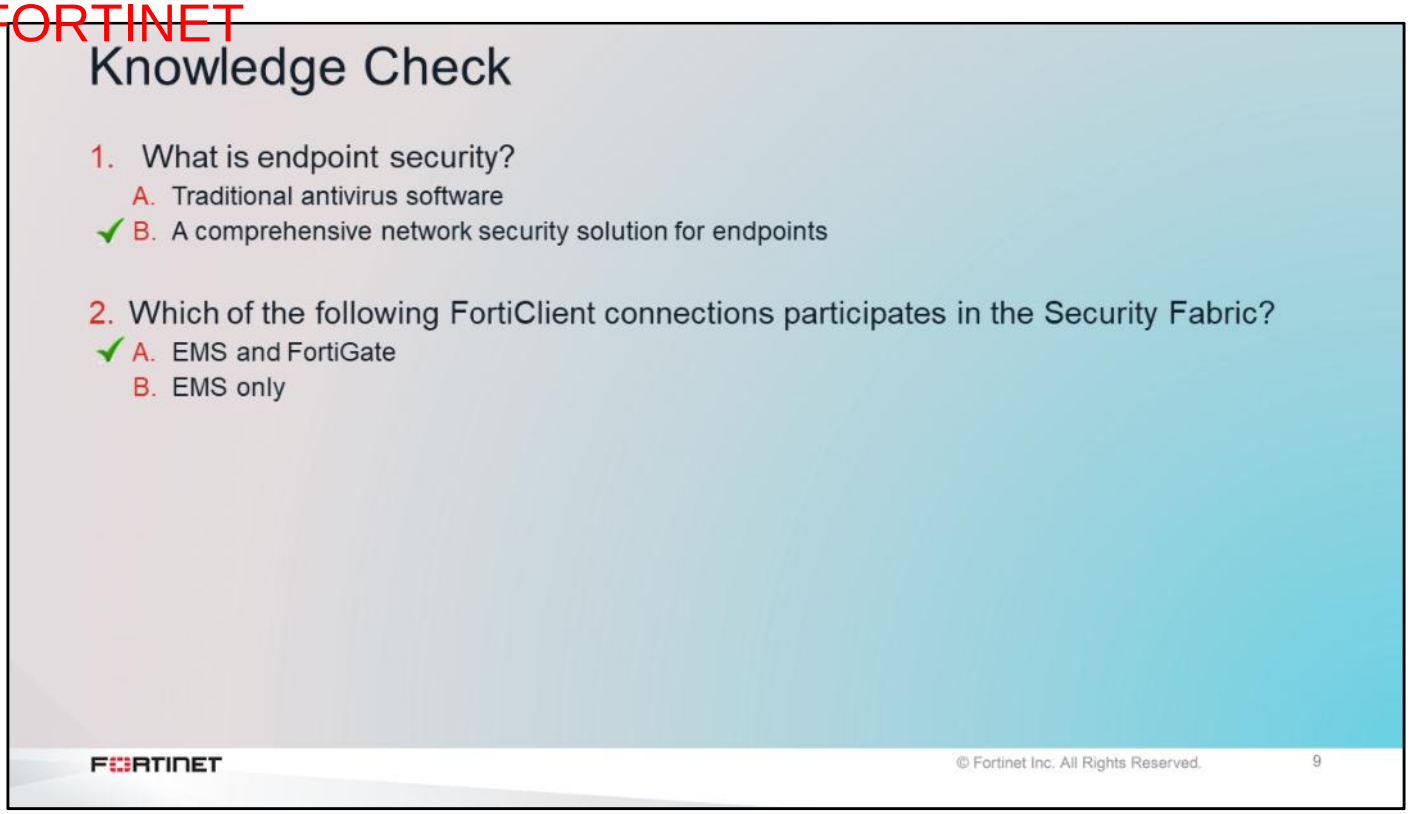
In 6.2.0, FortiClient must be used with EMS. FortiClient must connect to EMS to activate its license and become provisioned by the endpoint profile that the administrator configured in EMS. You cannot use any FortiClient features until FortiClient is connected to EMS and licensed.

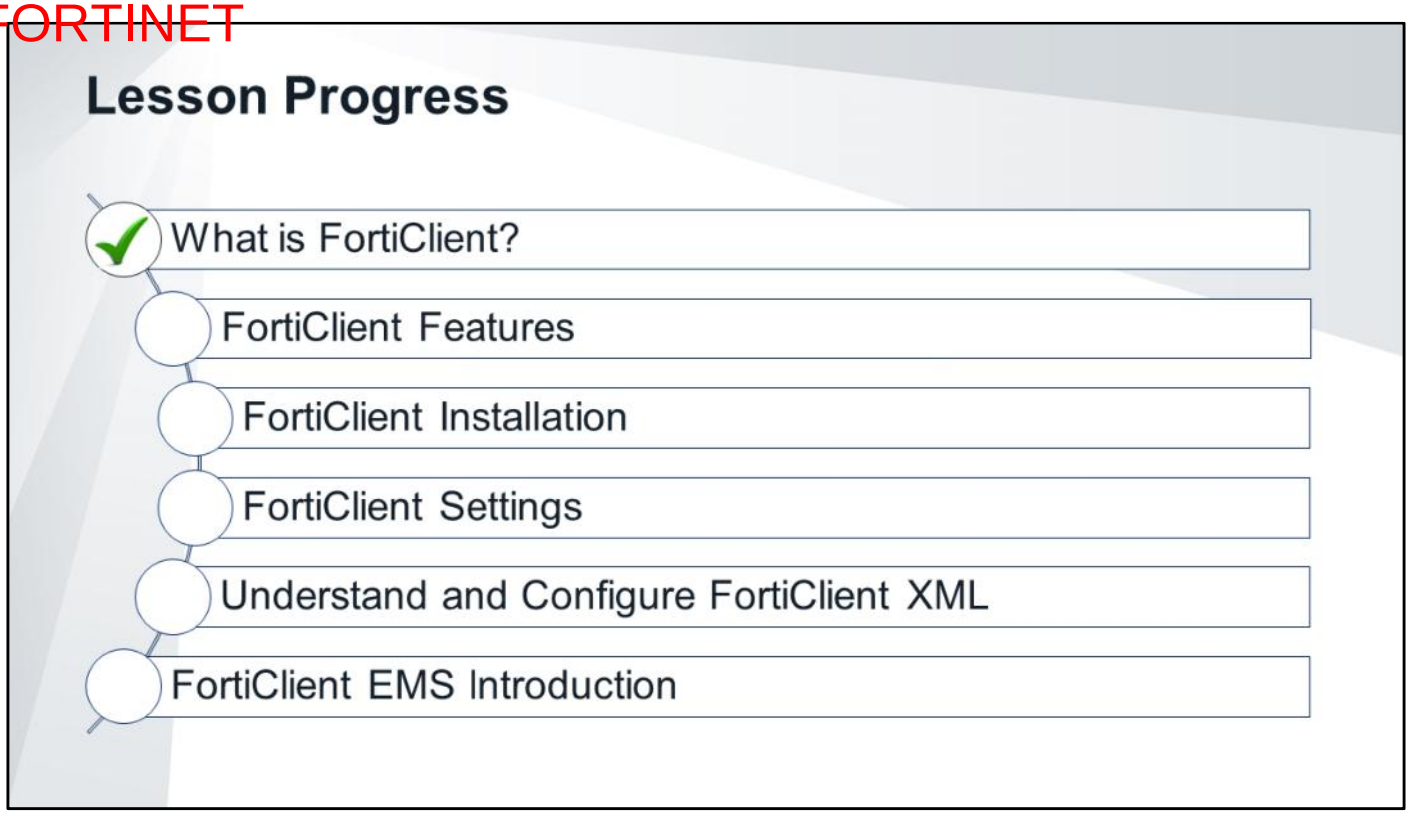
When FortiClient is connected only to EMS, EMS manages FortiClient. However, FortiClient cannot participate in the Fortinet Security Fabric.

When connected to EMS and a FortiGate, FortiClient integrates with the Security Fabric to provide endpoint awareness, compliance, and enforcement by sharing endpoint telemetry.

FortiClient automates prevention of known and unknown threats through its built-in host-based security stack and integration with FortiSandbox.

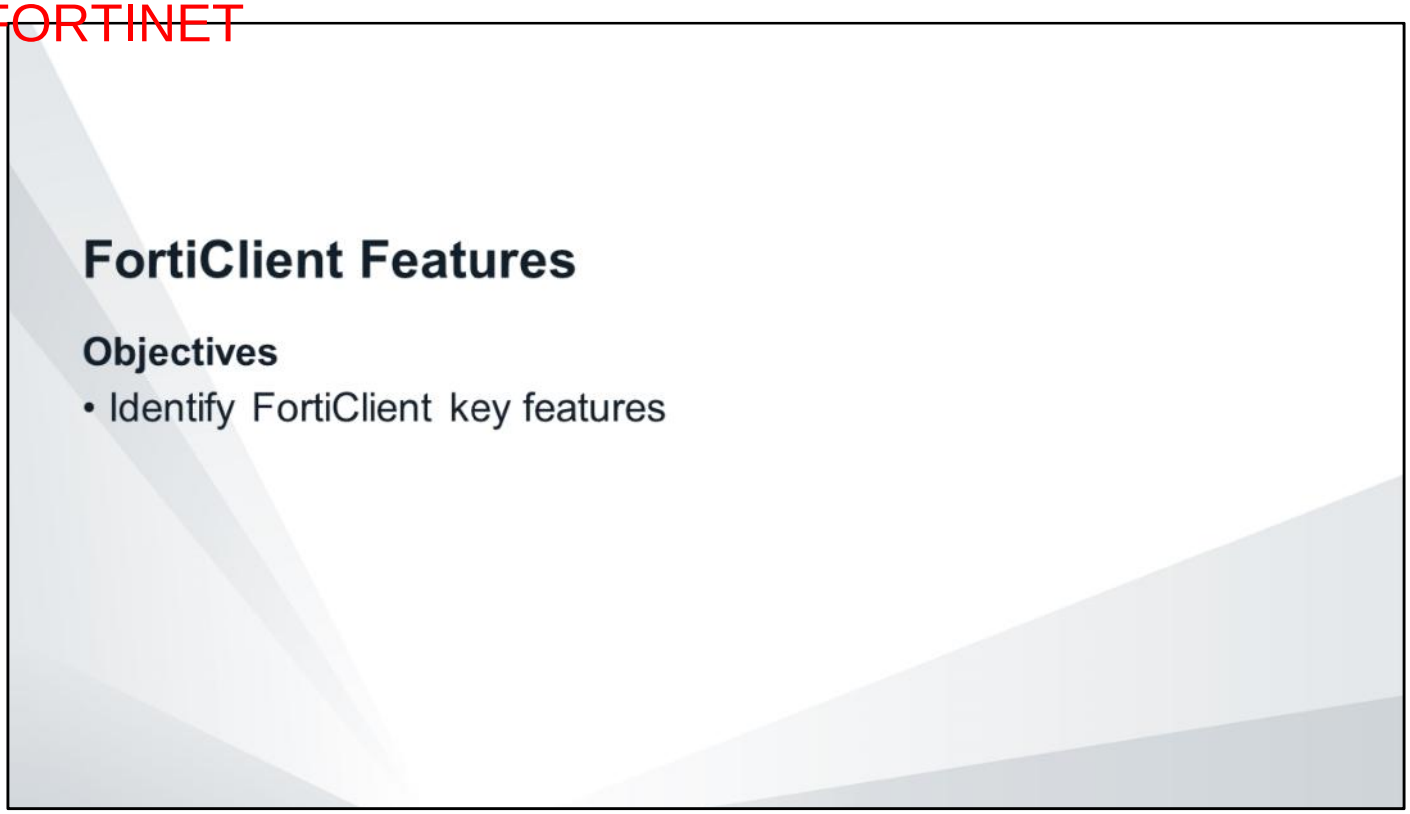
FortiClient also provides secure remote access to corporate assets through VPN.





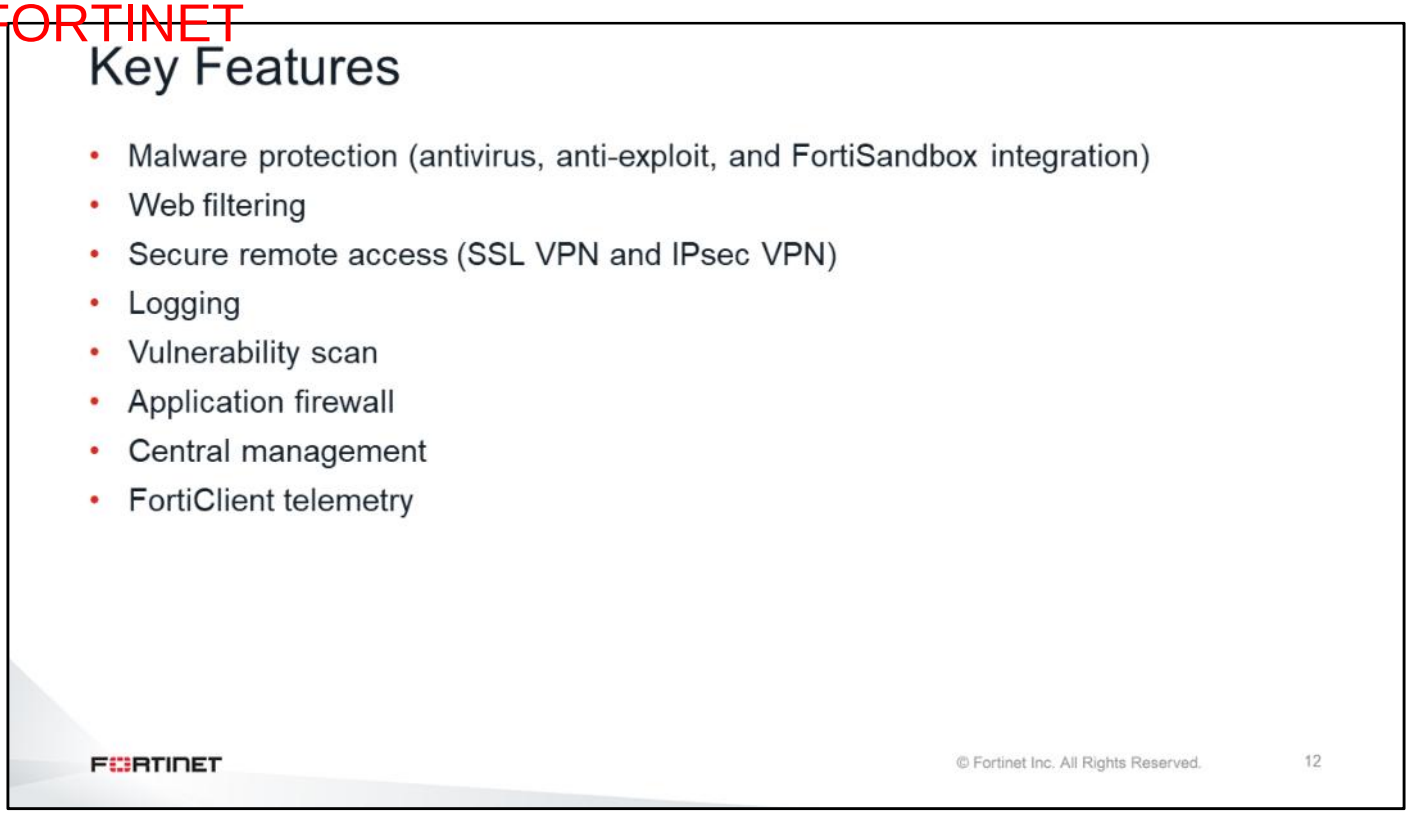
Good job! You now know more about what FortiClient is and what it does.

Now, you will learn about FortiClient features and what they do.



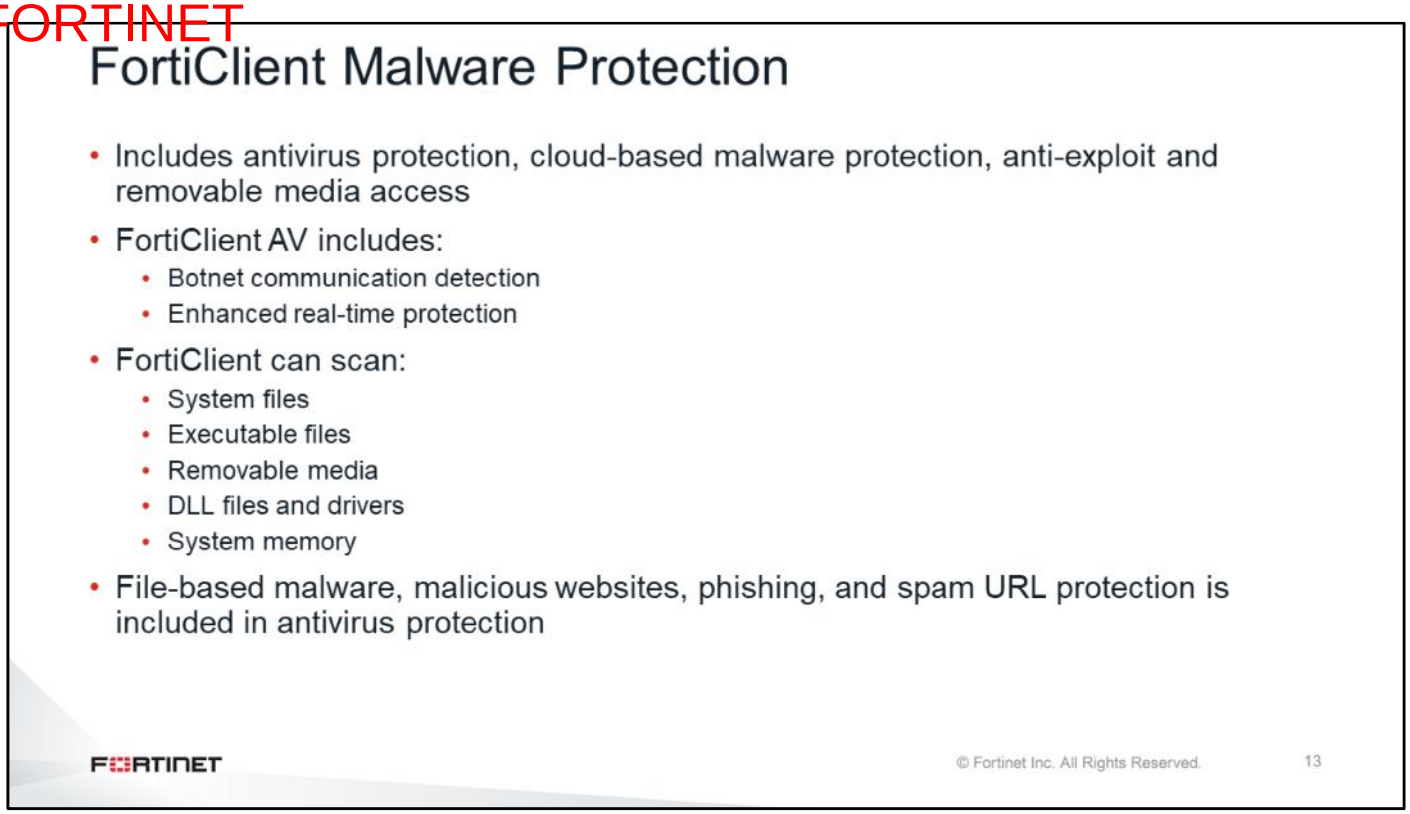
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in understanding the key features of FortiClient, you will be able to use FortiClient features and operation modes in your network.



FortiClient key features are shown on this slide.

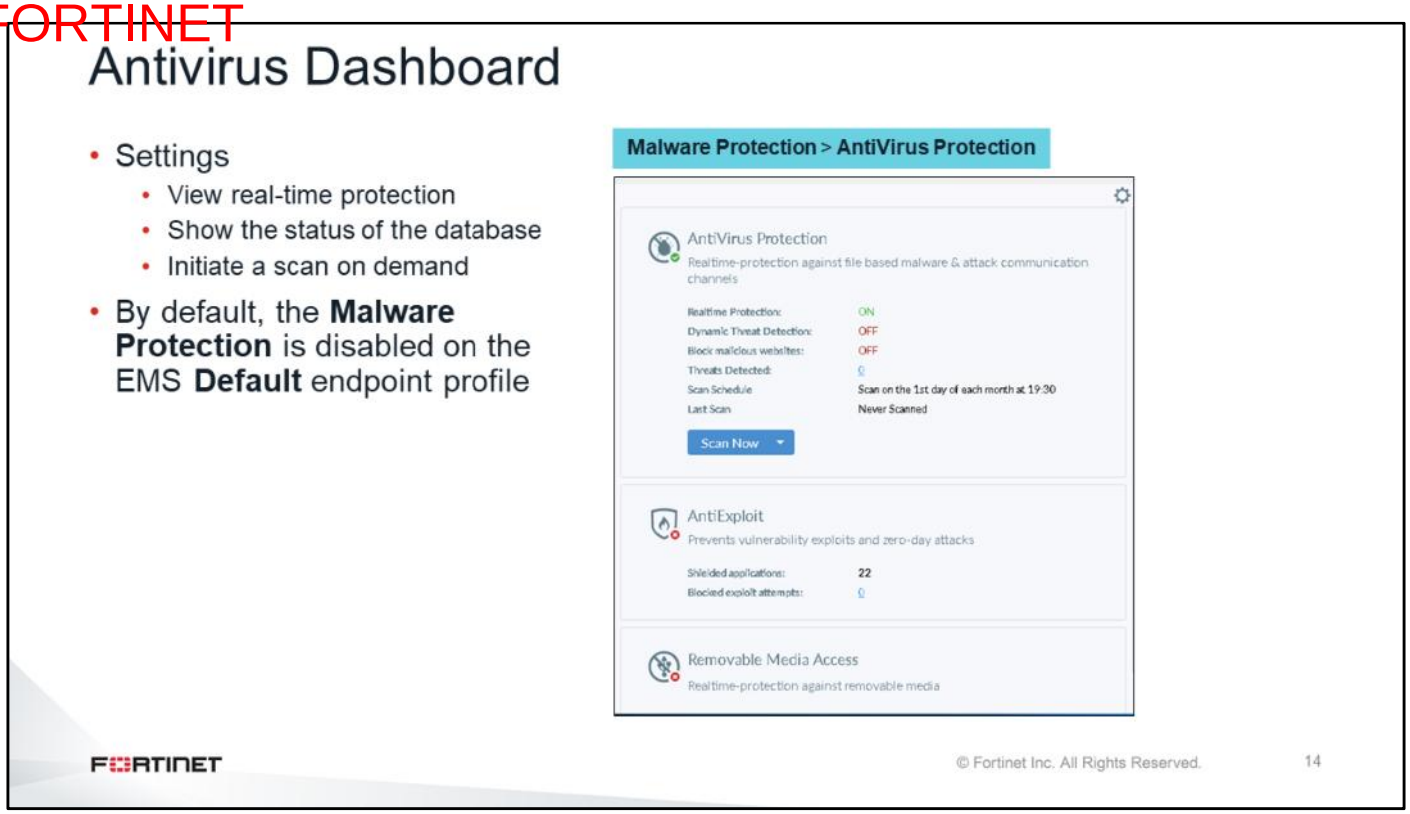
Note that, FortiClient requires a license. FortiClient licensing is applied to EMS.



FortiClient has enhanced capabilities for the detection of APT with FortiSandbox integration. These enhanced capabilities include:

- **Botnet command and control communications detection**: When you enable the botnet feature, FortiClient monitors and compares network traffic on a compromised system with a list of known command and control servers, and blocks it.
- **Enhanced real-time protection implementation (Windows only)**: The real-time protection (RTP) feature on FortiClient uses tight integration with Microsoft Windows to monitor files locally or over a network file system, as they are being downloaded, saved, run, copied, renamed, opened, or written to.

FortiClient can scan system files, executable files, removable media, dynamic-link library (DLL) files, memory, and drivers. FortiClient also scans for and remove rootkits. File-based malware, malicious websites, phishing, and spam URL protection is part of the antivirus component.

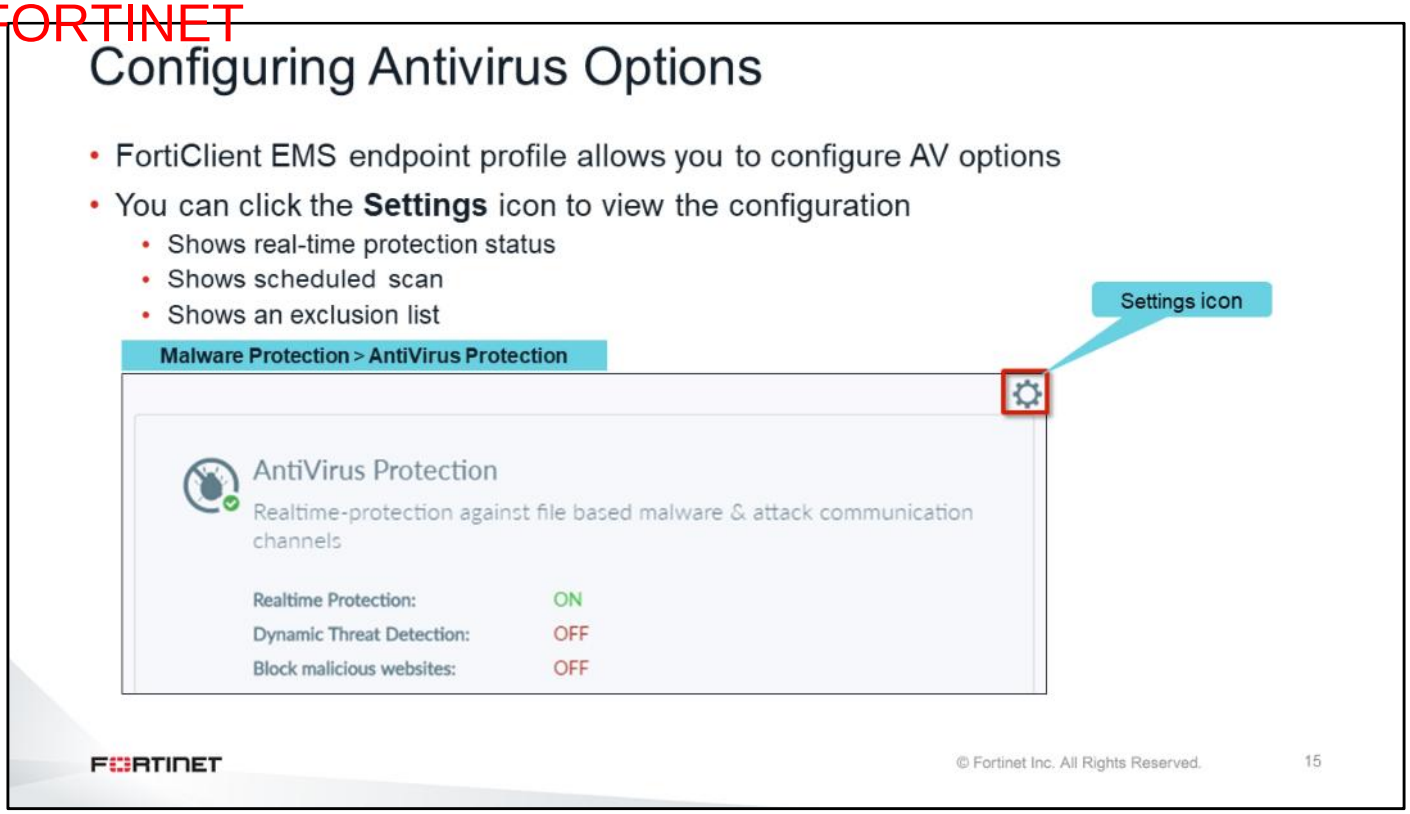


Now that you know more about the antivirus capabilities on FortiClient, you will learn more about the available antivirus options.

You can view the real-time protection status, view if the database is up-to-date, or perform an on-demand antivirus scan. Malware protection is disabled, by default, on the EMS **Default** endpoint profile. When the endpoint registers with the other endpoint profile, it receives the customized settings configured on that endpoint profile.

You will learn more about each of these options in detail in this lesson.

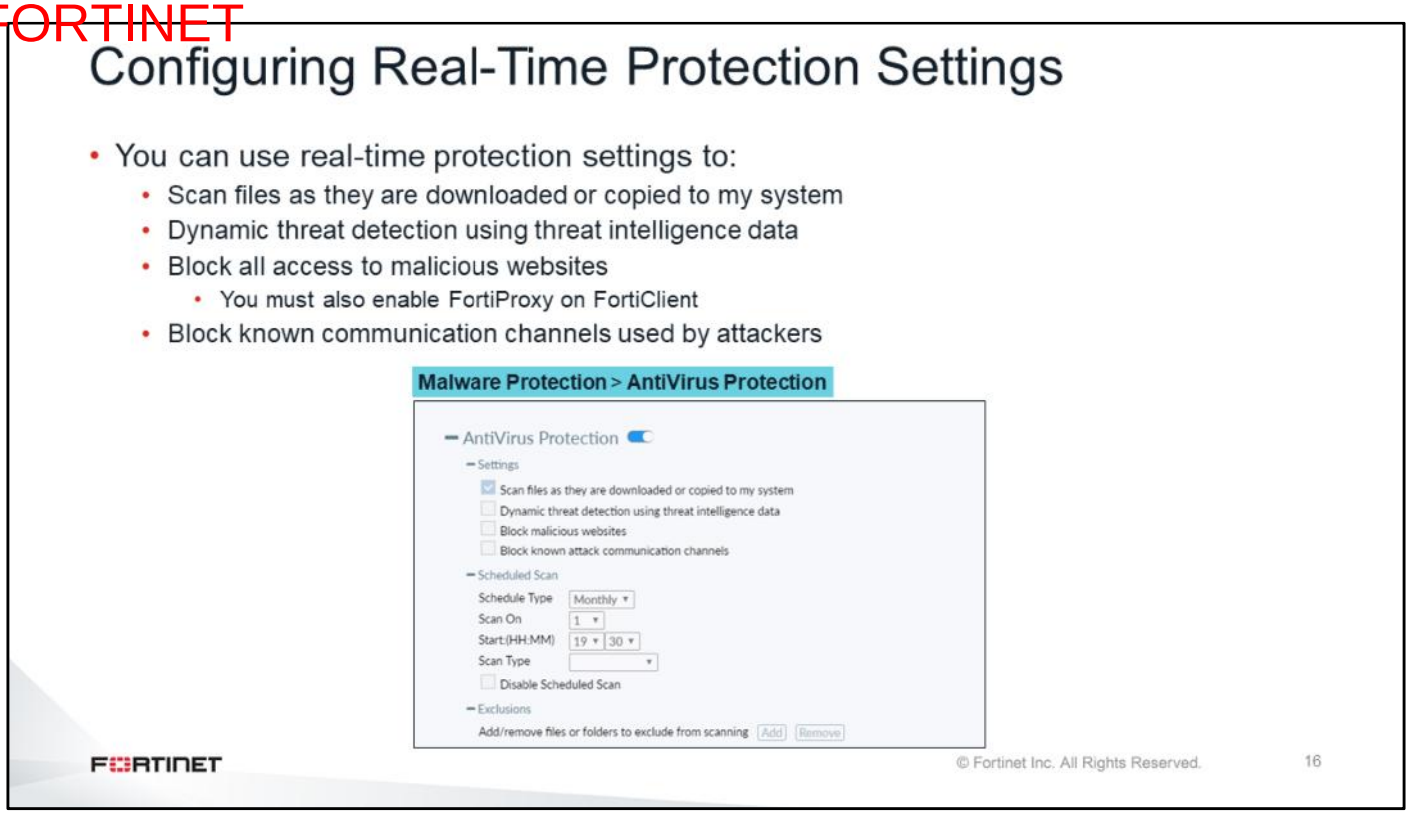
FortiClient automatically disables RTP after installation when one of the following is true:
- The OS is a server
- Exchange Server is detected
- SQL Server is detected



FortiClient security features are licensed with EMS. Without a connection to EMS, the features disappear. You can only configure AV options on an endpoint profile in EMS to make changes.

You can click the **Settings** icon to view most of the antivirus configuration. These options include:

- **Realtime Protection**: You can configure settings to specify what to scan. When a virus is detected during real-time monitoring, it will be automatically quarantined. If you have another antivirus program installed, FortiClient will display a warning message stating that your system may lock up or become unstable because of conflicts between the different antivirus products. You should uninstall all conflicting antivirus software before installing FortiClient or enabling antivirus real-time protection.
- **Scheduled Scan**: You can enable scheduled antivirus scans that will automatically scan your workstation at a scheduled time.
- **Exclusions**: You can create an exclusion list that includes files and folders that you don't want included in an antivirus scan.



You can select or clear the real-time protection settings in the EMS endpoint profile. This slide shows the options available on the FortiClient real-time protection. To enable real-time protection, you must select **Scan files as they are downloaded or copied to my system**. Why?

When you download software from the Internet, there is always a chance that you could download applications or programs that will try to inject malware, grayware, or viruses into your system.

You can also enable Command and Control (C&C) detection using IP reputation database signatures. It checks network traffic against known C&C IP addresses, plus port number combinations.

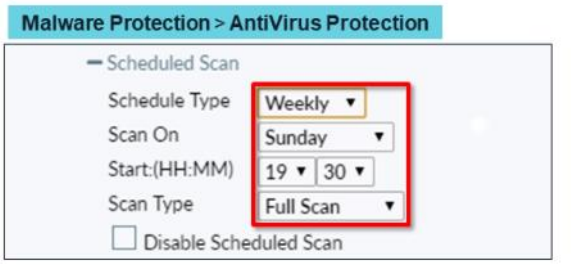
Block Access to Malicious Websites blocks all access to malicious websites. You must select **FortiProxy(Disable Only When Troubleshooting)** on the **System Settings** tab before you can enable this option.

You can configure one of the actions for the **Security Risk** site category, which includes block, warn, allow, and monitor. You can also select to view all the subcategories, and configure individual actions (Block, Warn, Allow, Monitor) for each subcategory. The security risk category contains the following subcategories:

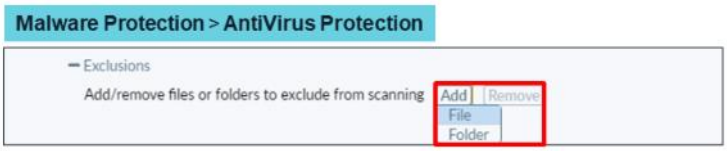
- Dynamic DNS
- Malicious Websites
- Newly Observed Domain
- Newly Registered Domain
- Phishing
- Spam URLs

Configuring Schedule Scan and Exclusions

- You can schedule scans to occur daily, weekly, or monthly and select from these scan types:
  - Quick Scan
  - Full Scan
  - Custom Scan



- You can create an exclusions list and add files and folders that will be excluded from the antivirus scan



FORTINET © Fortinet Inc. All Rights Reserved. 17

You can configure daily, weekly, and monthly scans as well as selecting one of the scan types on this slide. Quick scan only scans executable files, DLLs, and drivers that are currently running for threats. Full scan performs a full system scan including all files, executable files, DLLs, and drivers for threats, and Custom scan allows you to select a specific file folder on your local hard disk drive (HDD) to scan for threats. All three scan types runs the rootkit detection engine to detect and remove rootkits.

By default, FortiClient is scheduled to run full system scans monthly. It is recommended that you run a full system scan on your endpoint, as specified by the default setting. Using the default settings provides the best balance between protecting your endpoint from network threats and supporting the best overall performance. If the default settings does not meet your needs, you can adjust and fine-tune the settings accordingly.

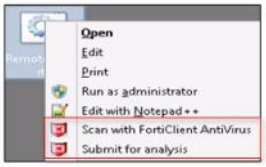
Note that if you configure monthly scans to occur on the 31st of each month, the scan will occur on the first day of the month for those months with less than 31 days.

If you want to exclude certain files or folders from the antivirus scan, but still want to perform an antivirus scan on the rest of the system, you can configure an exclusions list. The files and folders that you add to this list will be excluded from antivirus scanning.

On-Demand Antivirus Scanning

- You can click the **Scan Now** button to view on-demand antivirus scanning. You can select from these scan types:
  - Custom Scan
  - Full Scan
  - Quick Scan
  - Removable Media Scan

- You can scan a specific file or folder and submit a file for analysis by right-clicking that file on your workstation
  - You can submit up to 5 files a day to FortiGuard for analysis
  - SMTP port is used to upload files



FORTINET

18

You can also run an on-demand antivirus scan. There are four types of scans:

1. **Custom Scan**: Runs the rootkit detection engine to detect and remove rootkits. It allows you to select a specific file folder on your local hard disk drive (HDD) to scan for threats.
2. **Full Scan**: Runs the rootkit detection engine to detect and remove rootkits. It then performs a full system scan of all files, executable files, DLLs, and drivers.
3. **Quick Scan**: Runs the rootkit detection engine to detect and remove rootkits. It scans only the following items for threats: executable files, DLLs, and drivers that are currently running.
4. **Removable Media Scan**: You cannot schedule a removable media scan. A full scan will scan removable media.

You can view the date of the last scan run. You can perform a virus scan on a specific file or folder on your workstation by right-clicking the file or folder and selecting **Scan with FortiClient AntiVirus** and **Submit for analysis**. You can submit up to five files per day to FortiGuard for analysis. FortiClient use SMTP port 25 to upload files. The port must be open on the network firewall. The FortiGuard team does not provide feedback for the files submitted, but creates signatures for the malicious files detected.

Note that the **Submit for Analysis** option is only available when you select an individual file.

View Threats Detected

- The **Threats Detected** link allows you to view:
  - Quarantined files
  - Site violations
  - Real-time protection events

- Viewing quarantined files allows you to view details, view logs, or submit the suspicious file to FortiGuard
- When you view site violations, you can view website violations and submit them for recategorization
- The **Realtime Protection** link opens the `realtime_scan.log`

FORTINET © Fortinet Inc. All Rights Reserved. 19

The **Threats Detected** link allows you to view quarantined threats, site violations, and real-time protection events. Each link provides further information about the threat or violation.

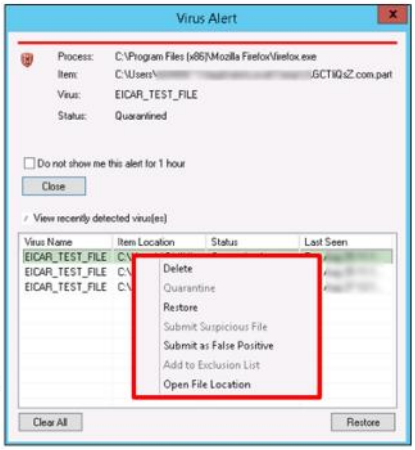
Quarantined Files link allows you to view, submit, or see details of the quarantined file. You can also view the original file location, view the virus name, submit the suspicious file to FortiGuard, and view logs. Only the EMS administrator can delete, whitelist, and restore quarantined files.

Site Violations link allows you to view site violations, which are part of FortiClient antivirus, and submit requests to have the site recategorized. It allows you to view site violation details, including the website name, category, date and time, user name, and status.

When an antivirus real-time protection event occurs, it is logged in `realtime_scan.log` and can be opened in any text editor. By default, real-time protection events open in the default viewer.

Virus Alert

- A warning message opens when a virus is detected while downloading a file through a web browser.
  - Deny access or quarantine the infected file
  - Right-click a file to access the context menu
- File action on quarantined file includes:
  - **Delete**: deletes a quarantined or restored file
  - **Quarantine**: quarantines a restored file
  - **Restore**: restores file and add to Exclusion list
  - **Submit Suspicious File**: submits a file to FortiGuard as a suspicious file
  - **Submit as False Positive**: submits a quarantined file to FortiGuard as a false positive
  - **Add to Exclusion List**: adds a restored file to the exclusion list
    - Any Files in the exclusion list will not be scanned
  - **Open File Location**: opens the file location on your workstation



FORTINET

20

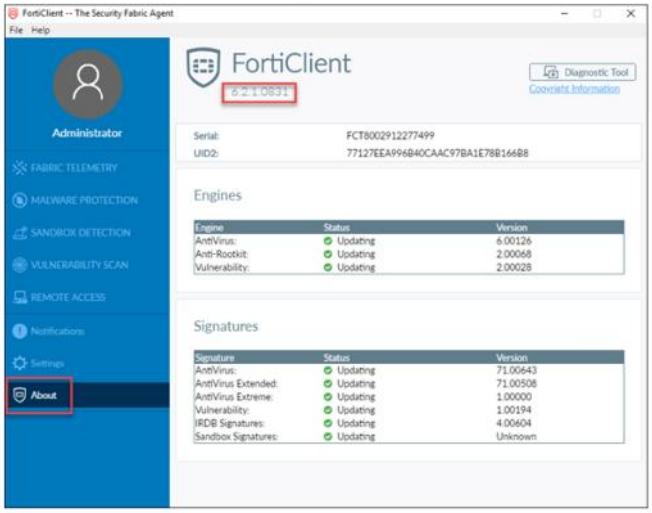
If FortiClient detects a virus file that is being downloaded through a web browser, FortiClient presents a warning message if the action on virus discovery is either set to **Deny Access To Infected File** or **Quarantine Infected File**. When the file discovery action is quarantined, you can take one of the actions shown on this slide. FortiClient locks the file on specified location shown in the file details page until any action is taken. In version 6.2, restore and whitelist is done on EMS quarantine management.

When the action is set to **Deny Access to Infected Files**, a message is displayed stating that users are not permitted to download the file as it is infected.

Note that if you do not select **Alert when viruses are detected**, the virus alert dialog box will not open when you attempt to download a file that contains a virus through a web browser.

FortiClient Engine and Signature Version

- You can view FortiClient engine and signature versions

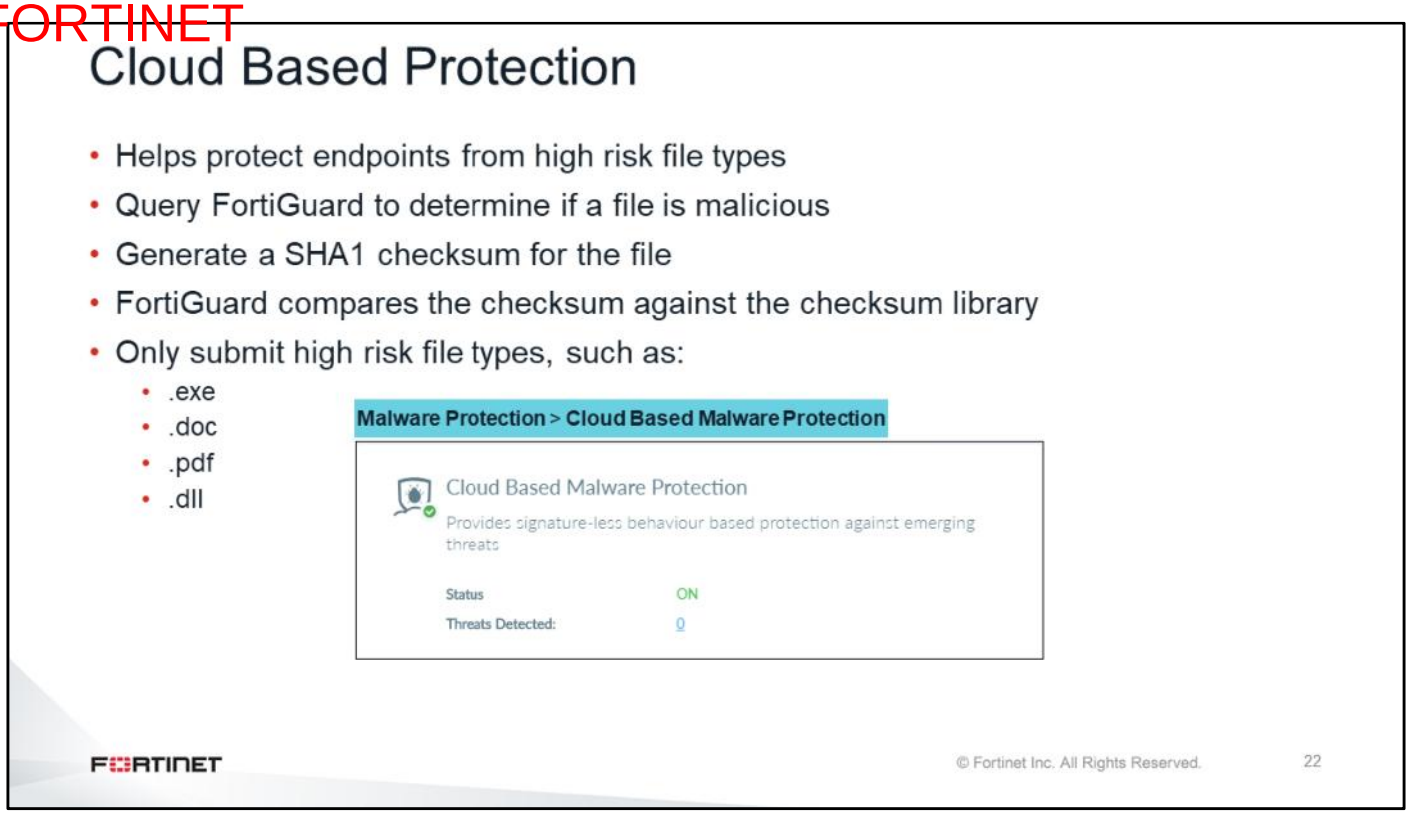


FORTINET

 21

You can view the current FortiClient version, engine, and signature information by selecting **About**.

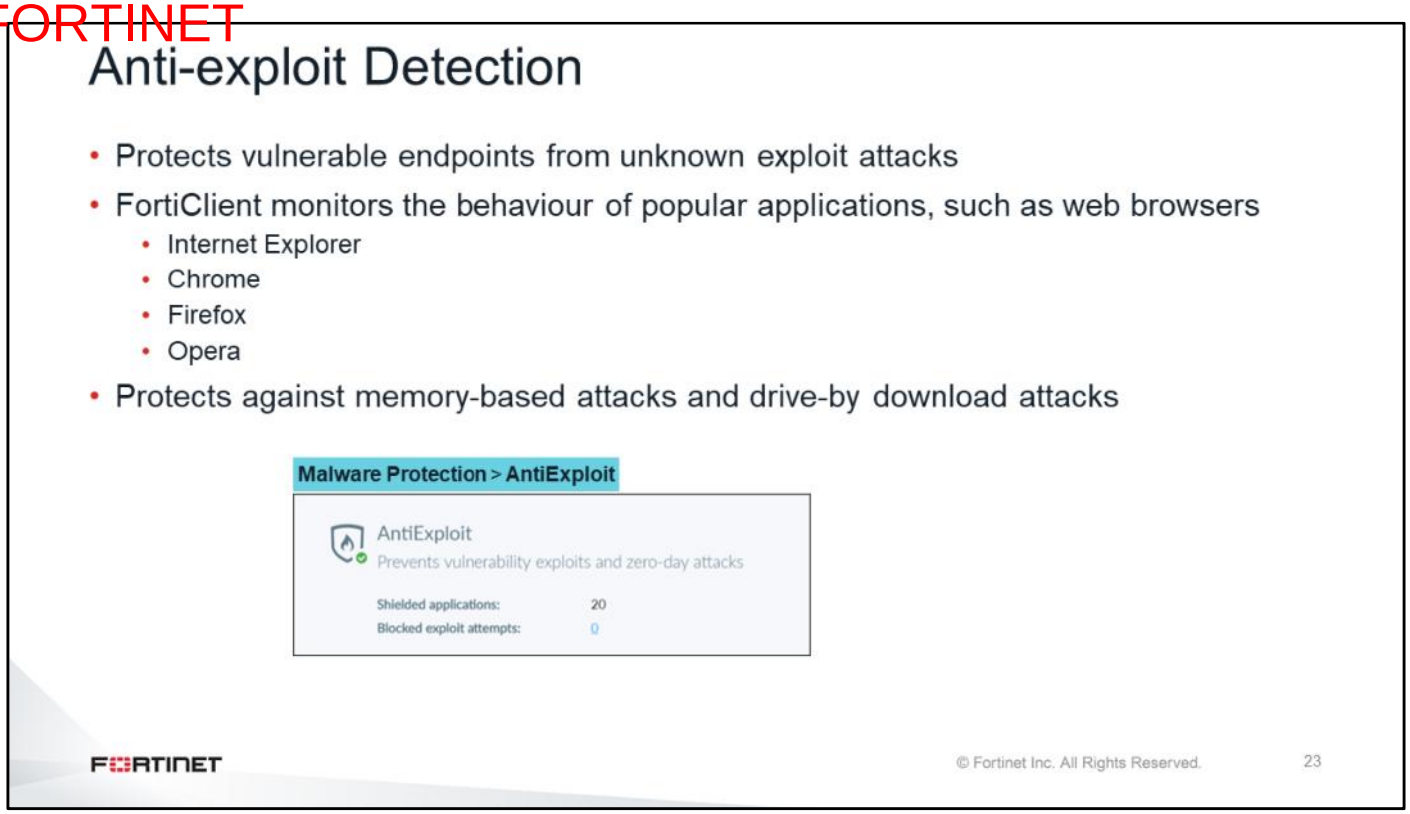
You can use FortiManager for client software and signature updates when registered on FortiGate or EMS.



The cloud-based malware protection feature helps protect endpoints from high risk file types from external sources, such as the Internet or network drives, by querying FortiGuard to identify whether files are malicious. When a file is downloaded or executed, FortiClient generates a SHA1 checksum for the file. FortiClient sends the checksum to FortiGuard , where it is compared against the FortiGuard checksum library to identify if it is malicious. If the checksum is found in the library, FortiGuard communicates to FortiClient that the file is deemed malware. By default, FortiClient quarantines the file.

This feature only submits high risk file types, such as .exe, .doc, .pdf, and .dll, to FortiGuard. You can enable this feature independently of antivirus protection.

The list of high risk file types is the same as the list of file types submitted to FortiSandbox by default.



The anti-exploit detection protects vulnerable endpoints from unknown exploit attacks. FortiClient monitors the behaviour of popular applications, such as web browsers (Internet Explorer, Chrome, Firefox, Opera), Java/Flash plug-ins, Microsoft Office applications, and PDF readers, to detect exploits that use zero-day or unpatched vulnerabilities to infect the endpoint. Once detected, FortiClient terminates the compromised application process.

The anti-exploit detection feature also protects the endpoint from memory-based attacks and drive-by download attacks. It also detects and blocks unknown and known exploit kits.

It is a signature less solution.

Anti-exploit Detection (Contd)

- You can view the exploit attempts FortiClient has blocked

- You can view applications protected from exploits

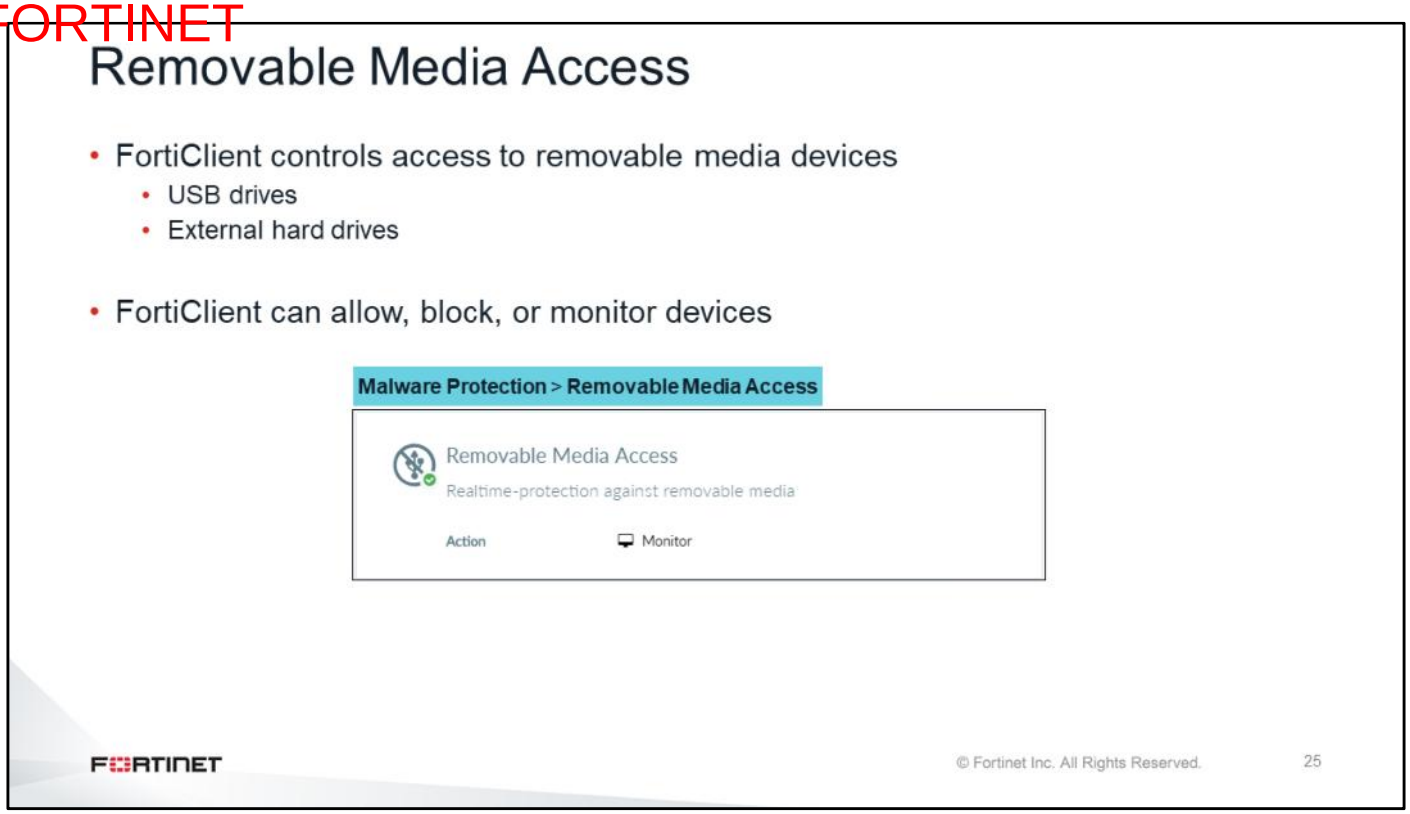
FORTINET

24

You can determine which applications are protected from exploits based on the buttons beside their names.

Applications with an **Exclude** button beside their names are protected from evasive exploits.

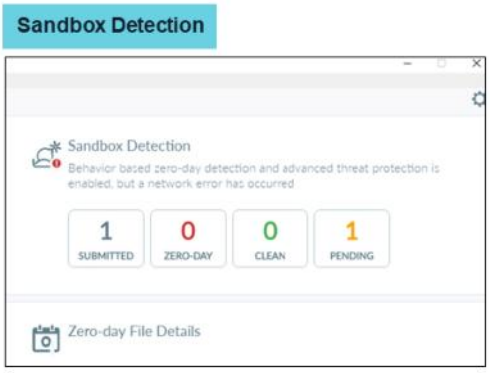
Applications with an **Unexclude** button beside their names are not protected from evasive exploits. You can protect the application by clicking the **Unexclude** button.



FortiClient controls access to removable media devices, such as USB drives or external hard drives. FortiClient can allow, block, or monitor access to removable media devices, as configured by the EMS administrator.

Sandbox Detection

- FortiClient supports integration with FortiSandbox
- FortiClient sends files to FortiSandbox for further analysis if they are not detected locally
- Endpoint users can also manually submit files to FortiSandbox for scanning
- Access to files can be blocked until the FortiSandbox scanning result is returned



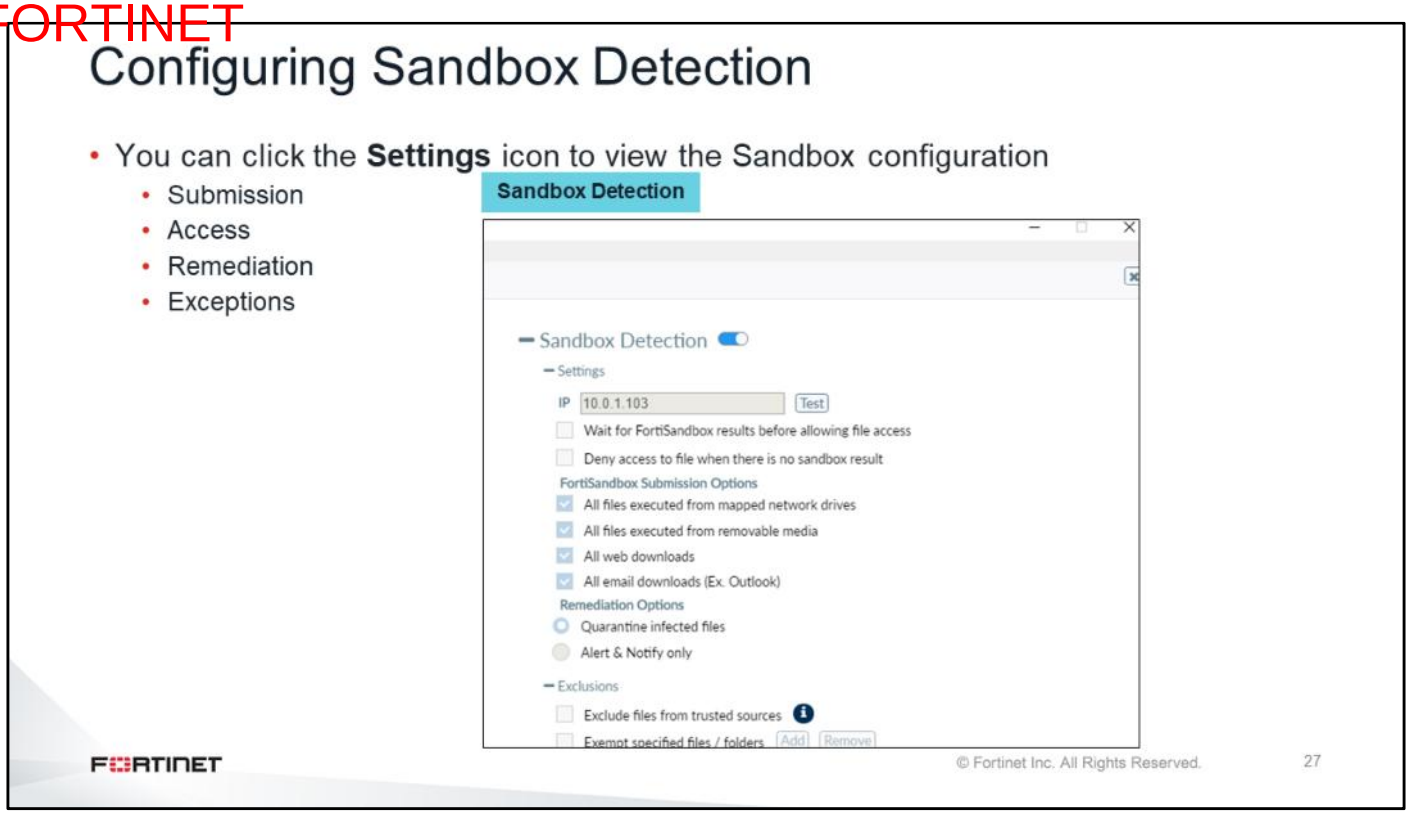
FORTINET

26

FortiClient supports integration with FortiSandbox. When configured, FortiSandbox automatically scans files downloaded on the endpoint, or from removable media attached to the endpoint, or mapped network drives. FortiClient also automatically scans files downloaded with an email client on the endpoints, or from the Internet.

In each case, if the file is not detected locally, and FortiSandbox integration is configured, FortiClient sends the file to the FortiSandbox for further analysis. Endpoint users can also manually submit files to FortiSandbox for scanning. Access to files can be blocked until the FortiSandbox scanning result is returned. When scanning is complete, FortiSandbox can quarantine infected files, or alert and notify the endpoint user of infected files without quarantining the files.

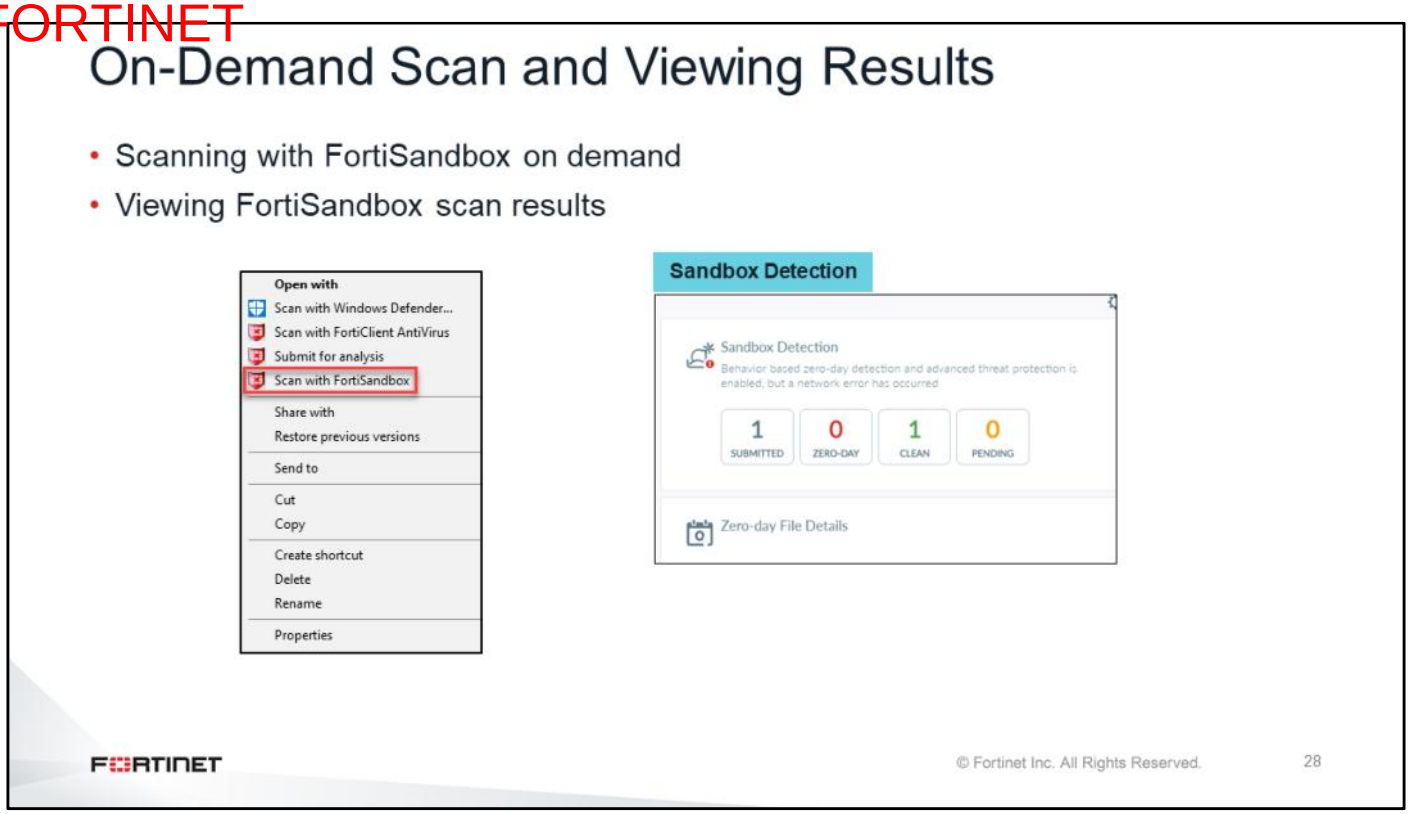
FortiClient periodically downloads the latest AV signatures from FortiSandbox, and applies them locally to all real-time and on-demand AV scanning. FortiClient can send a maximum of 300 files daily to FortiSandbox Cloud. If multiple files are submitted around the same time, FortiClient sends one file to FortiSandbox Cloud, waits until it receives the verdict for that file, then sends the next file to FortiSandbox Cloud. In case of FortiSandbox appliance, total number of files send by FortiClient is limited to hardware specifications.



You can click the **Settings** icon to view the sandbox configuration. These options include:
Wait for FortiSandbox results before allowing file access: Select to wait for FortiSandbox analysis results before files can be accessed.
Deny Access to file when there is no sandbox result: Select to deny access to files when FortiClient cannot reach FortiSandbox for file analysis or no result.
You can view the following FortiSandbox submission options:
All files executed from mapped network drives: Select to submit all files that are executed on mapped network drives to FortiSandbox for analysis. Clear the check box to disable this feature.
All files executed from removable media: Select to submit all files executed on removable media, such as USB drives, to FortiSandbox for analysis. Clear the check box to disable this feature.
All web downloads: Select to submit all web downloads on the endpoint to FortiSandbox for analysis
All email downloads (Ex. Outlook): Select to submit all email downloads on the endpoint to FortiSandbox for analysis.
You can view the following remediation options:
Quarantine infected files: Select to quarantine infected files.
Alert & Notify only: Select to alert and notify the endpoint user about infected files, but not quarantine infected files.
You can view the following exclusion options:
Exclude files from trusted sources: Select to exclude files from trusted sources from FortiSandbox analysis.

- **Exempt specified files / folders:** Select to exempt specified files and/or folders from FortiSandbox analysis. You must also create the exclusion list.

Note that all the configuration changes are done on the EMS endpoint profile. For example, you can also include files with no extension but it needs to be configured through XML configuration.



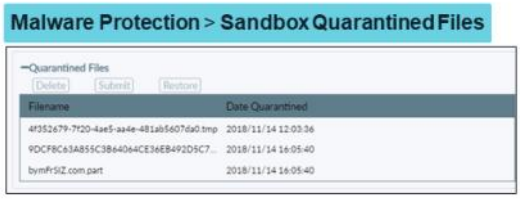
You can send files to FortiSandbox for scanning on demand when FortiSandbox is enabled and online.

FortiSandbox scan results display on the **Malware Protection** page. When a virus is detected, FortiClient creates a notification alert that displays the number of files.

Submitted box shows the number of files submitted to FortiSandbox for scanning. Zero-day box shows the number of detected zero-day files. Clean box shows the number of files determined clean after FortiSandbox scanning, and pending box shows the number of files waiting for FortiSandbox scanning.

View, Submit, Restore, and Delete Quarantined Files

- Endpoint user can view files quarantined by FortiSandbox
- Endpoint user can also see details of quarantined files and submit them for another analysis

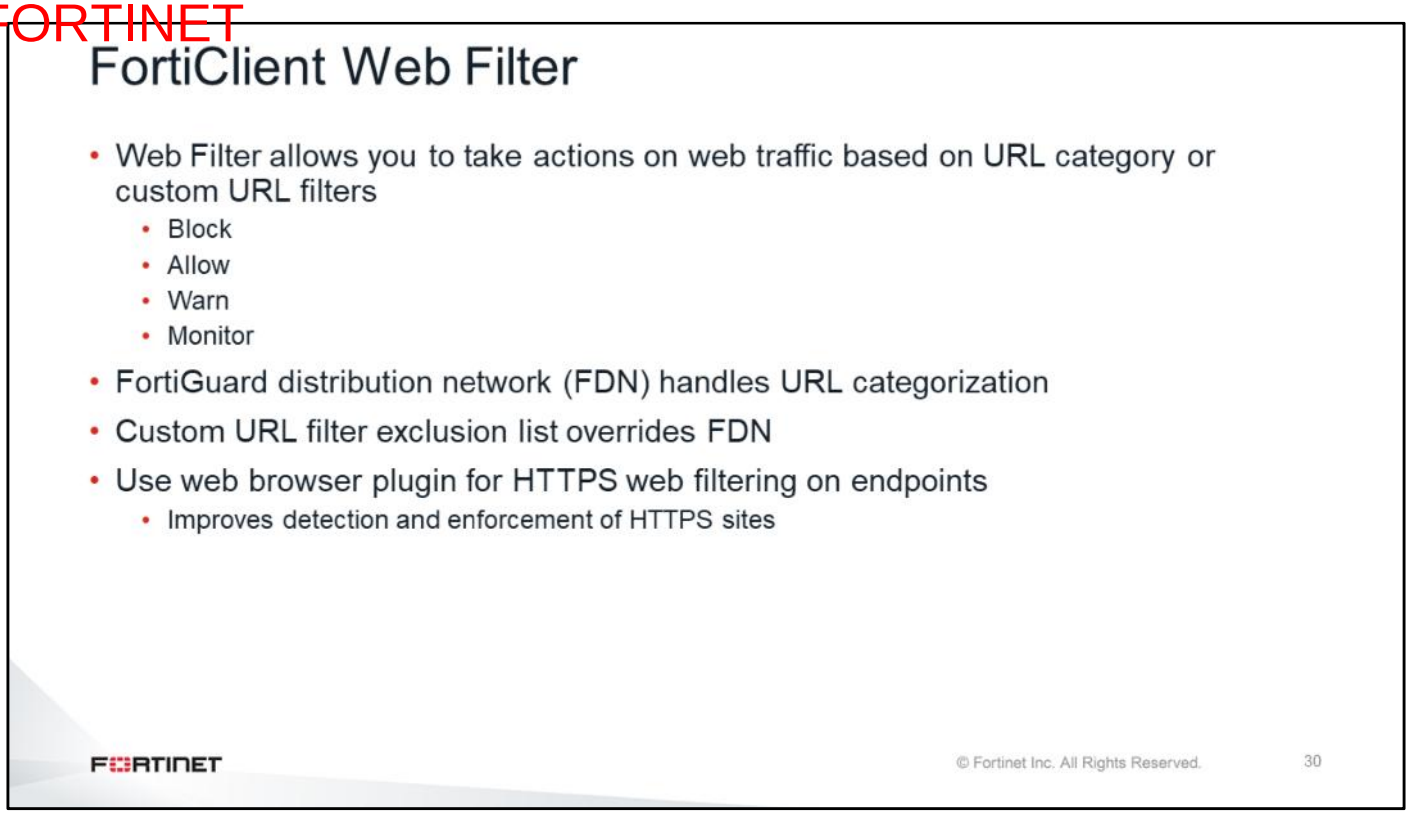


FORTINET © Fortinet Inc. All Rights Reserved. 29

You can view files quarantined by FortiSandbox. Endpoint users can only submit files to FortiSandbox for scanning and checking details of quarantined files.

The maximum age for quarantined files is specified in the `<quarantine></quarantine>` XML tags.

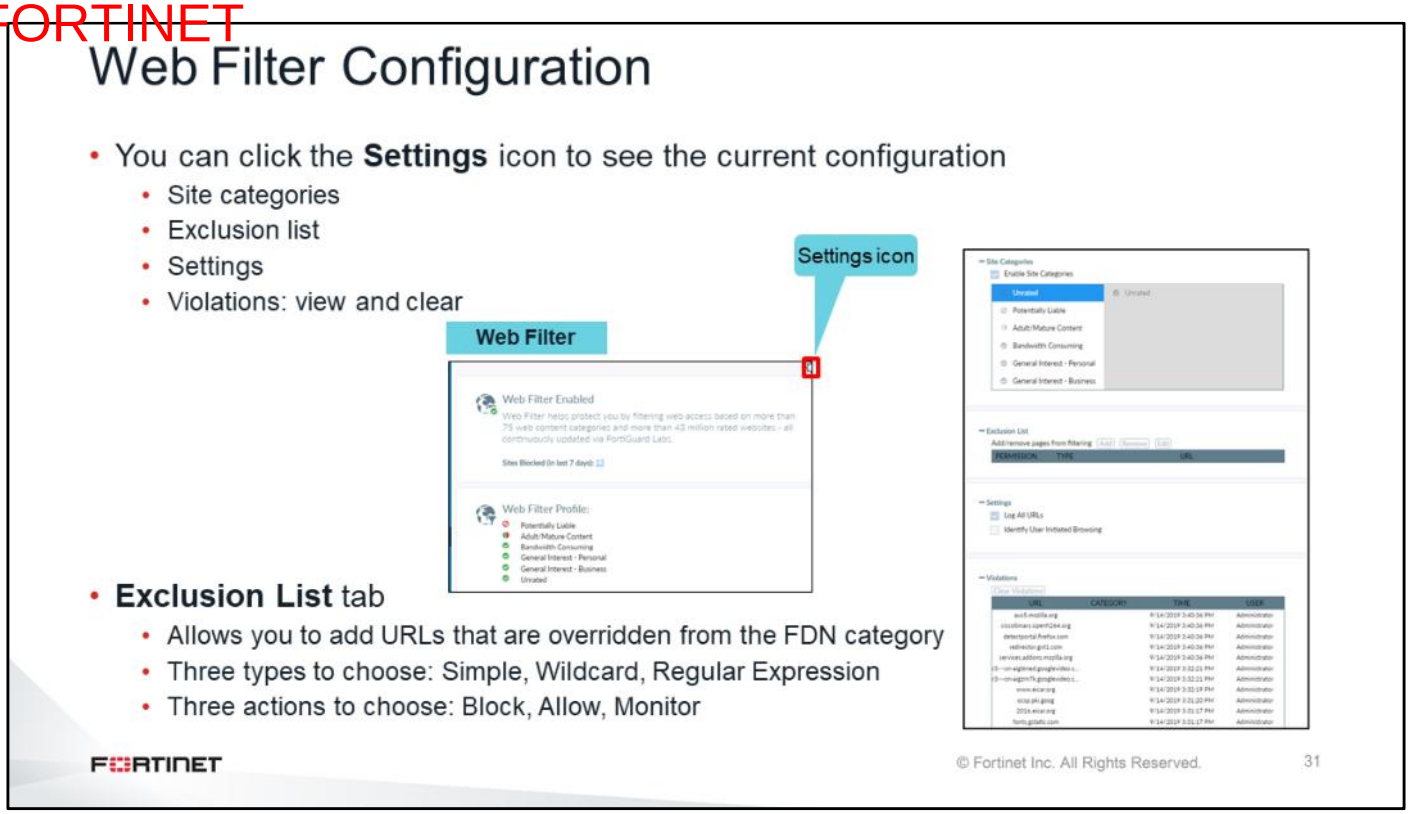
FortiClient sends quarantined file information to EMS. If the EMS administrator whitelists the file (in the case of a false positive), EMS sends the whitelist information to FortiClient. After FortiClient receives the whitelist information, it releases the file from quarantine.



After FortiClient is registered to EMS, web filter configuration settings are pushed from the management device and are read only on the FortiClient console.

Web filter features allow you to block, allow, warn, and monitor web traffic based on URL category or custom URL filters. URL categorization is handled by the FDN. You can create a custom URL filter exclusion list which overrides the FDN category.

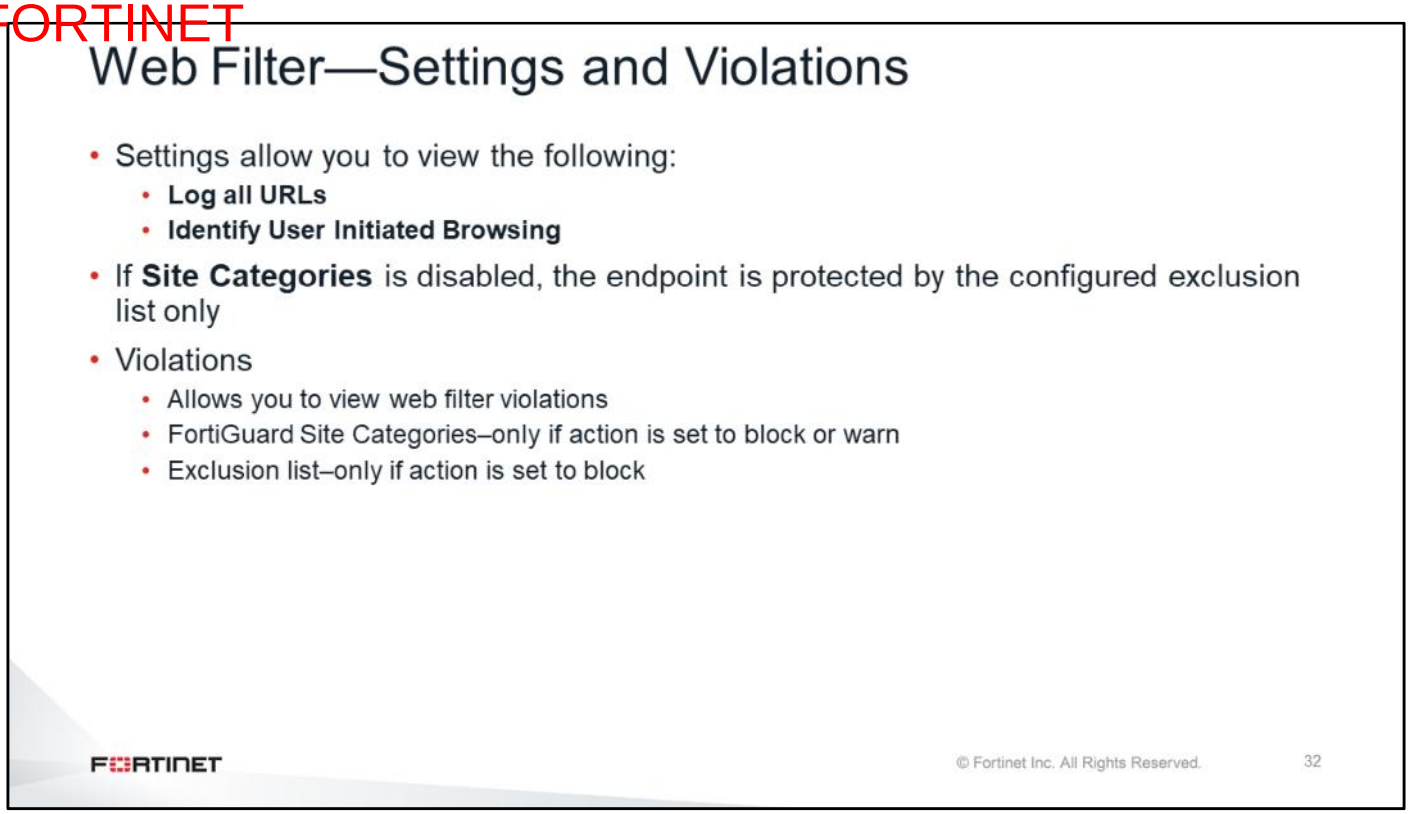
The EMS administrator can enable a web browser plugin for HTTPS web filtering on the endpoint. This improves detection and enforcement of Web Filter rules on HTTPS sites. After this option is enabled, you must open the browser to approve installing the new plugin. The plugin is only supported for the Google Chrome browser on Windows platforms.



The EMS administrator can configure web filter on the EMS endpoint profile Web filter tab. Configurable options include web security profile (site categories), exclusion list, settings, and violations.

The endpoint user can view current configuration by clicking the settings icon. The EMS administrator can configure a web security profile to **Allow**, **Block**, **Warn**, or **Monitor** web traffic based on website categories and subcategories.
Allow: Permits access to the sites within the category.
Block: Prevents access to sites within the category. Users attempting to access a blocked site will receive a replacement message explaining that access to the site is blocked.
Warn: Presents the user with a message, allowing them to continue if they choose. Accepting a disclaimer will allow users to browser the override category for 5 minutes.
Monitor: Permits and logs access to sites in the category. You may also enable user quotas when enabling the monitor action.

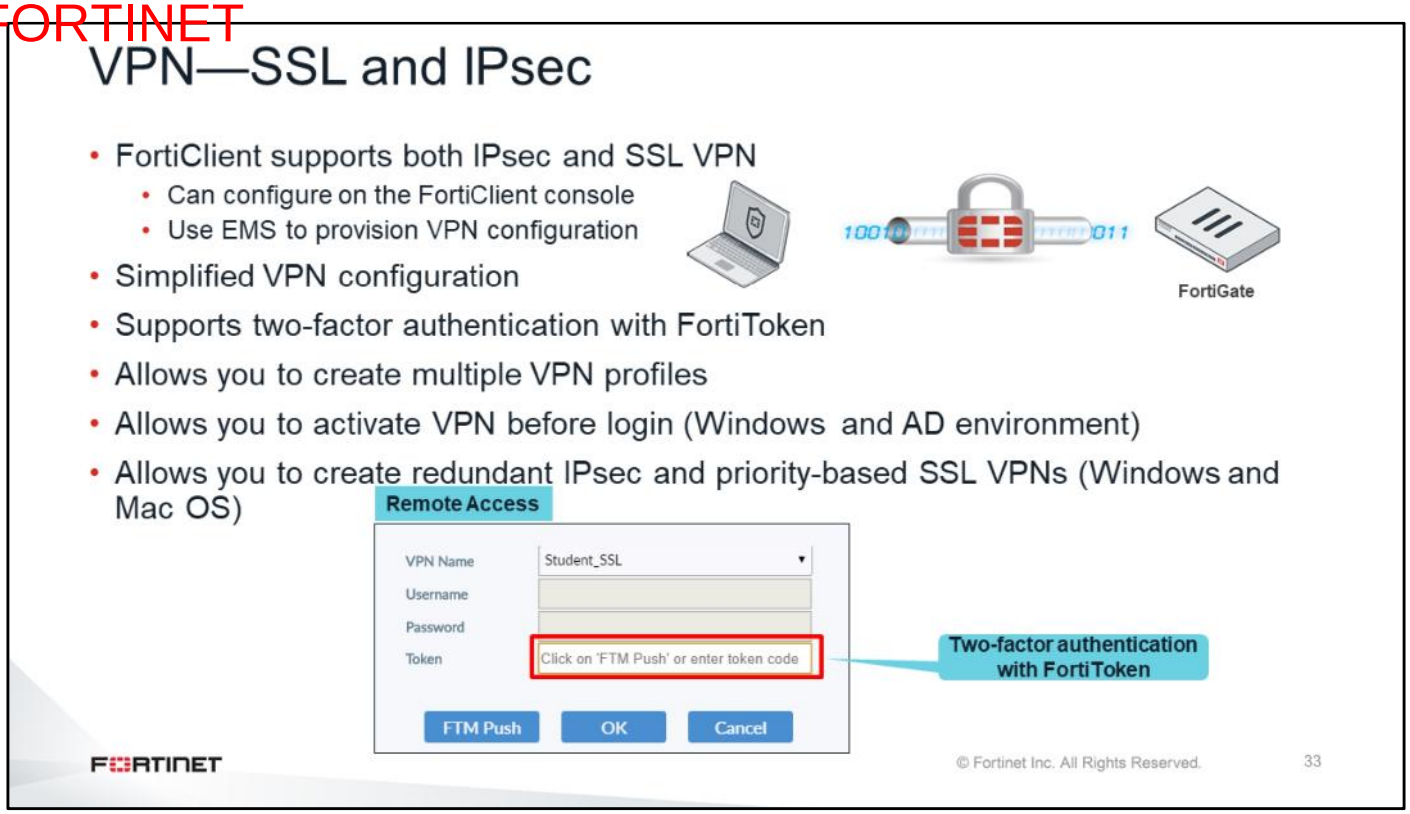
What if you want to exempt a URL that is part of a category, but you still want to take action on that category as a whole?
The EMS administrator can configure an exclusion list to which admin can add websites and set the permissions to allow, block, and monitor. An admin can also configure simple, wildcard, or regular expressions as a type. If the website is part of a blocked category, an allow or monitor permission in the exclusion lists allows the user to access the specific URL.



When you configure web filter general settings, you can choose to log all URLS with an assigned action, and the logged files can be downloaded. You can also select to log only user initiated browsing.

Note that when site categories are disabled, FortiClient is protected by the exclusion list only.

You can view site violations and violation details, including the website name, category, date and time, and username. The violation will show only if the action is set to **block** or **warn** for FortiGuard site categories, and **block** for the exclusion list.



FortiClient supports both IPsec and SSL VPN connections to your network for remote access. EMS administrator can provision client VPN connections in the FortiClient profile (EMS endpoint profile) or the endpoint user can configure new connections in the FortiClient console.

You can also configure two-factor authentication using FortiToken for enhanced security for both types of VPNs on your FortiGate device for FortiClient VPN connections.

FortiClient VPN features are not limited to basic configuration and provisioning, but can be used for advanced configurations. For example, you can automatically connect to a VPN when FortiClient is launched, or you can map or unmap a network drive when a tunnel is connected or disconnected, respectively.

You can also configure FortiClient to connect to a VPN before the login in (either logging in to a Windows account, or through an AD environment). Advanced features like redundant IPsec VPN and priority-based SSL VPN are also supported on FortiClient for Windows and Mac OS.

IPsec VPN

- Easy configuration to create, edit, or delete VPN connections
  - Authentication settings–prompt on login, save login (only username), or disable
  - Allows you to configure VPN settings, phase I, and phase II settings
- Configure many advanced configurations when managed by FortiGate or FortiClient EMS
  - Redundant IPsec VPN connections
  - Save password
  - Auto connect
  - Always up

FORTINET © Fortinet Inc. All Rights Reserved. 34

You can configure the IPsec VPN directly on the FortiClient console when EMS administrator allows you to add personal VPN connections. This allows you to create, edit, save, or delete IPsec VPN connections. You can create and save multiple IPsec connections. Because this configuration is one side of the IPsec VPN, the configuration settings must match with the FortiGate IPsec configuration in order to connect and access remote resources.

When personal VPN is not allowed by the FortiClient EMS administrator, the endpoint profile VPN tab allows you to provision these configurations, along with advanced configurations, such as redundant IPsec VPN connections, save password, auto connect, and always up, to name a few.

SSL VPN

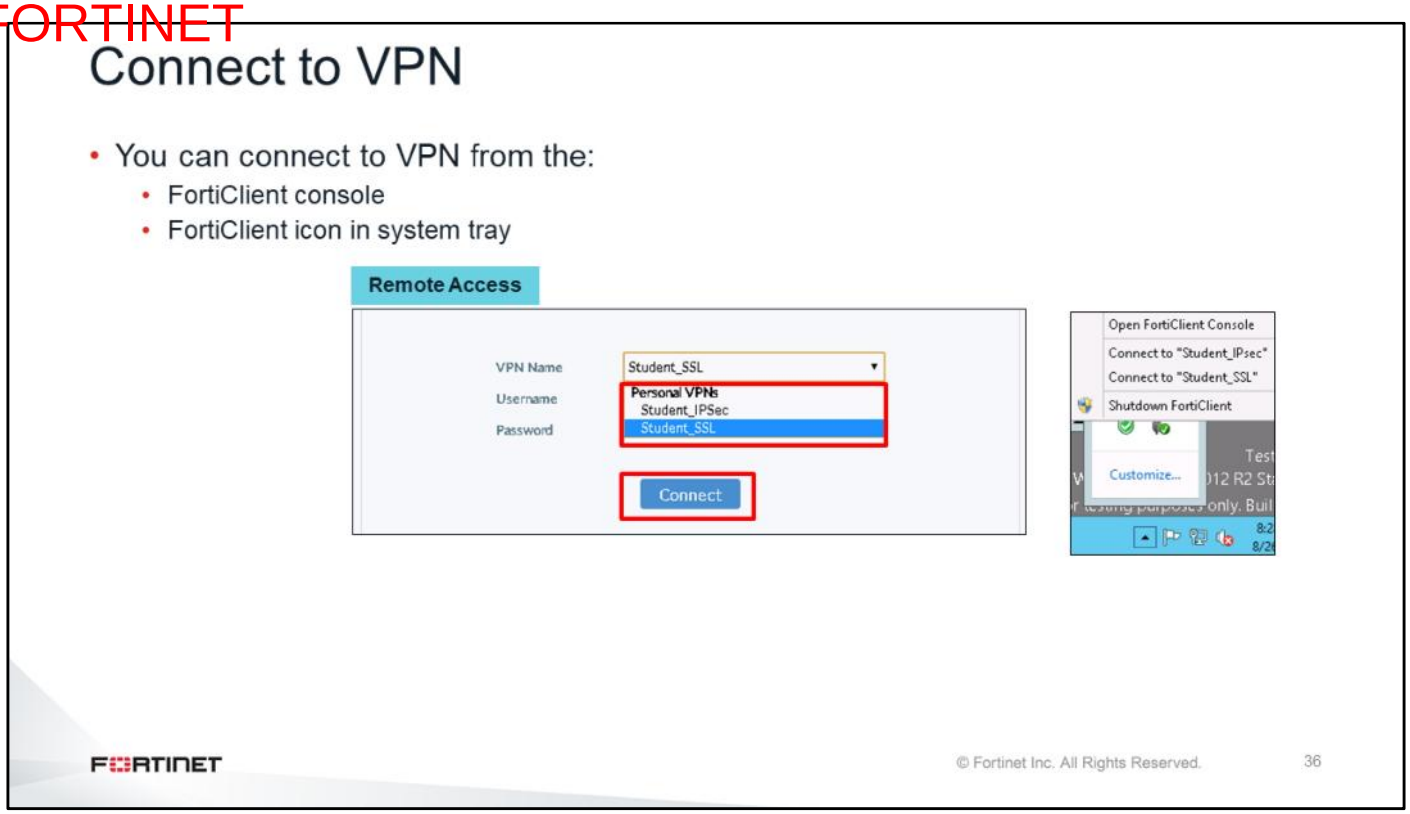
- Create, edit, or delete a VPN connection
  - Save the login information–username
  - Configure authentication–prompt on login, save login (only username), or disable (only when **Client Certificate** option is enabled)
- When managed by FortiClient EMS, perform advanced configuration:
  - Priority-based SSL VPN connections
  - SSL VPN portal on FortiGate allows:
    - Save password
    - Auto connect
    - Always up
- Supports DTLS
  - If required, falls back to TCP over TLS
  - Windows only

35

The SSL VPN configuration is similar to the IPsec configuration, where you configure one side of the tunnel and the other side is configured on FortiGate.

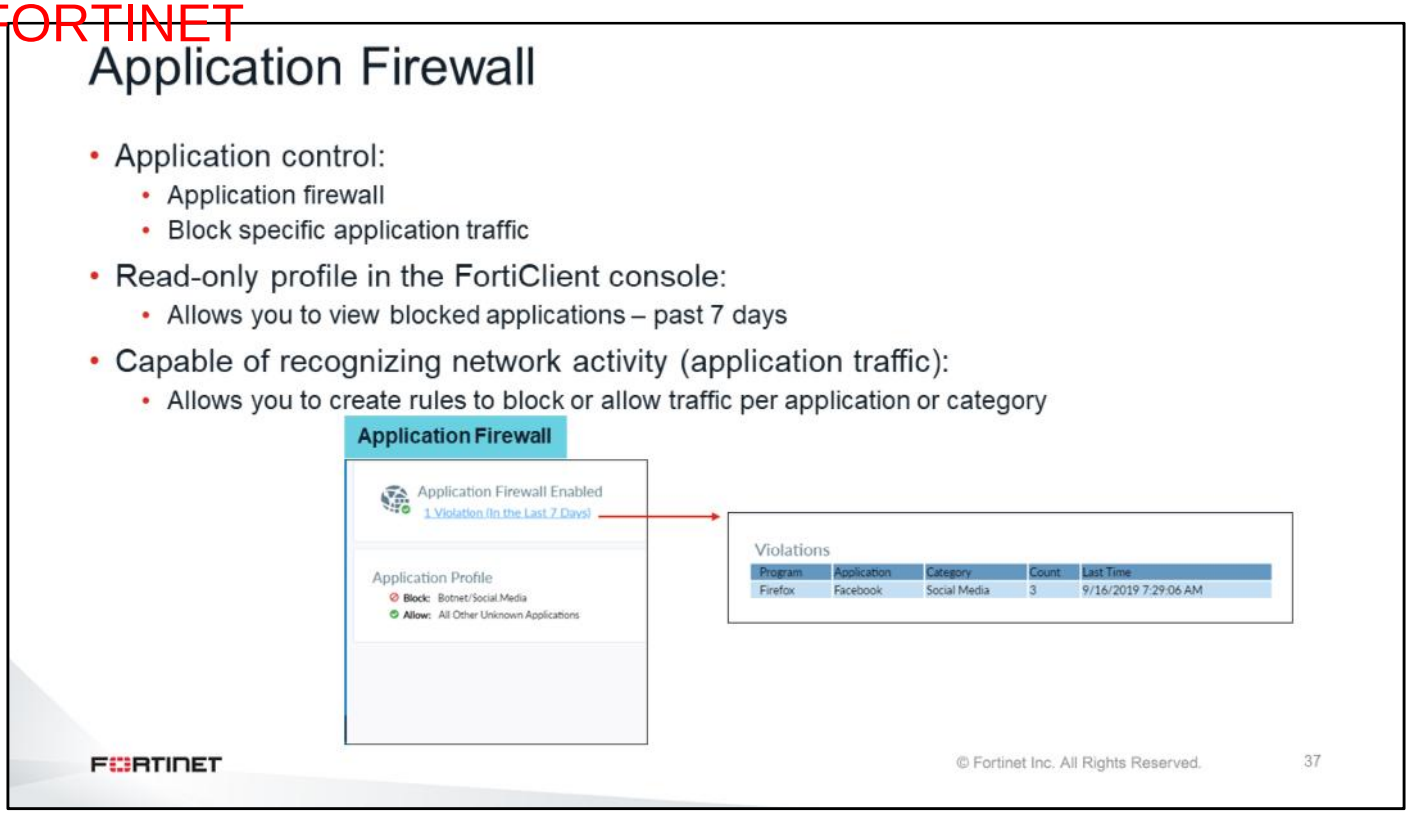
When personal VPN is not allowed by the FortiClient EMS administrator, endpoint profile VPN tab allows you to provision these configurations, along with advanced configurations on SSL VPN portals, and many more.

DTLS is a Windows-only feature, and not recommended for slower networks. DTLS settings must also be enabled on FortiGate SSL VPN settings.



To connect to a VPN (IPsec or SSL), select the VPN name from the drop-down list on the FortiClient console. Enter your username, password, and then click **Connect**. Optionally, in the system tray, right-click the FortiClient icon and select the VPN connection you want to connect to. When connected, the console will display the connection status, duration, and other relevant information.

Note that provisioned VPN connections will be listed under **Corporate VPN**. Locally configured VPN connections will be listed under **Personal VPN**.

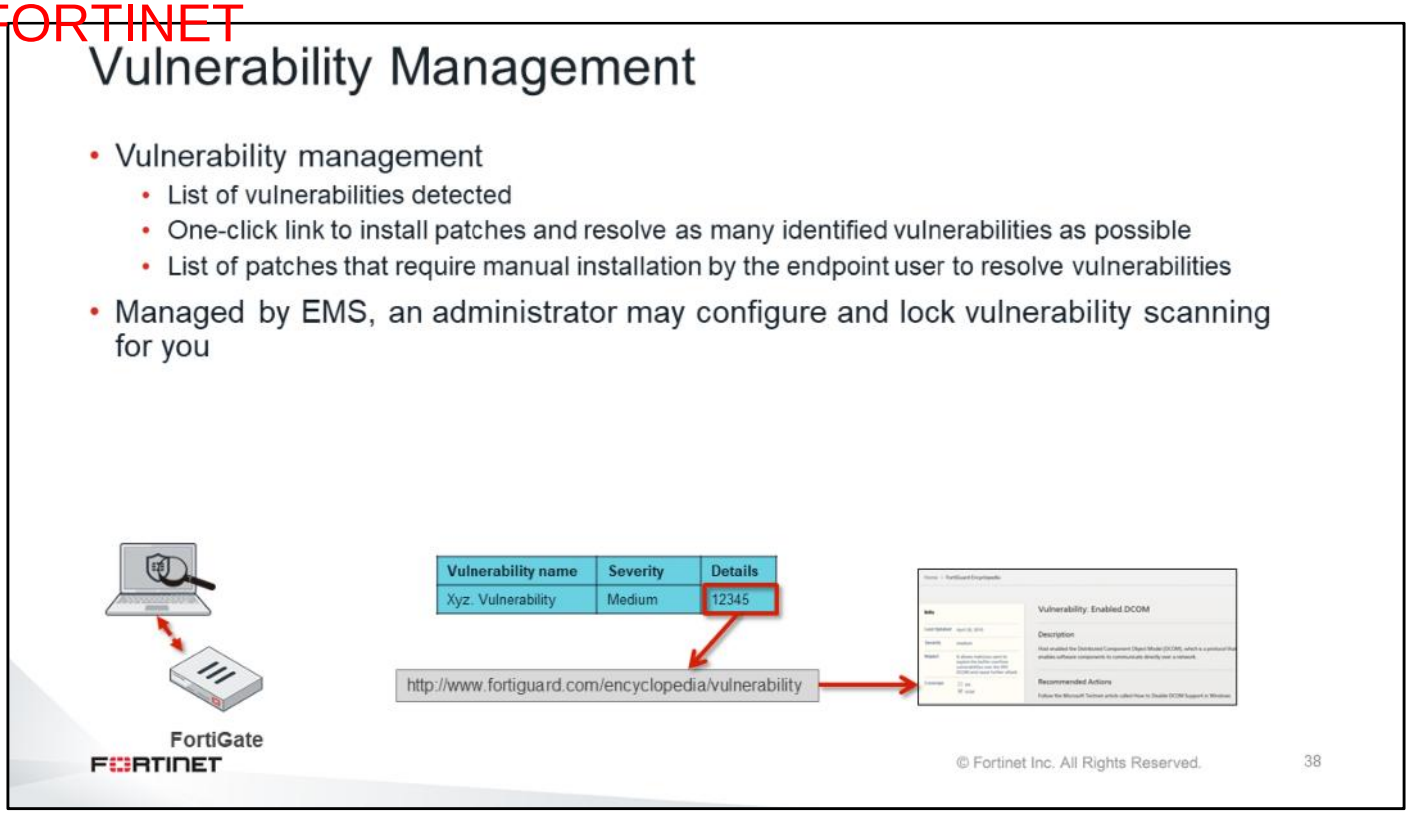


You can use the application firewall feature to detect and take actions against network traffic, depending on the application that is generating the traffic.

The application firewall uses IPS protocol decoders to analyze and detect application traffic, even on non-standard ports.

FortiClient can recognize the traffic generated by a large number of applications. You can create rules to block or allow application traffic on FortiGate or EMS, based on the category or application. The rules are then pushed to managed FortiClient.

Application firewall settings are read-only on the FortiClient console. You can view blocked applications for the past seven days.

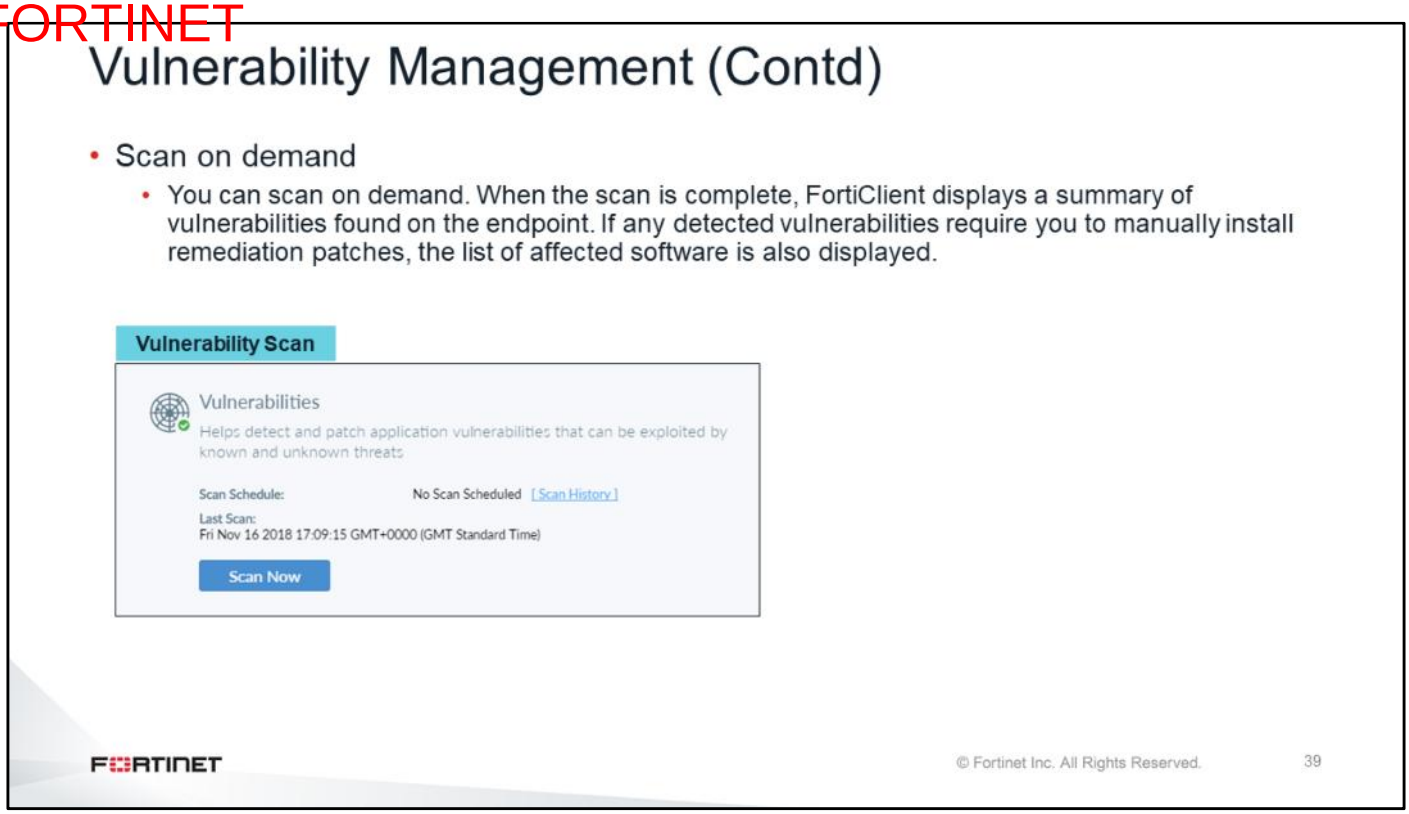


When endpoint users are transferring data over the Internet, hackers can exploit vulnerabilities in endpoint devices, and use those vulnerabilities to gain unauthorized access to the system.

FortiClient can perform a vulnerability scan to search endpoint devices to identify weaknesses, provide details about the impact of those weaknesses and recommend actions to protect the applications running on the endpoint devices.

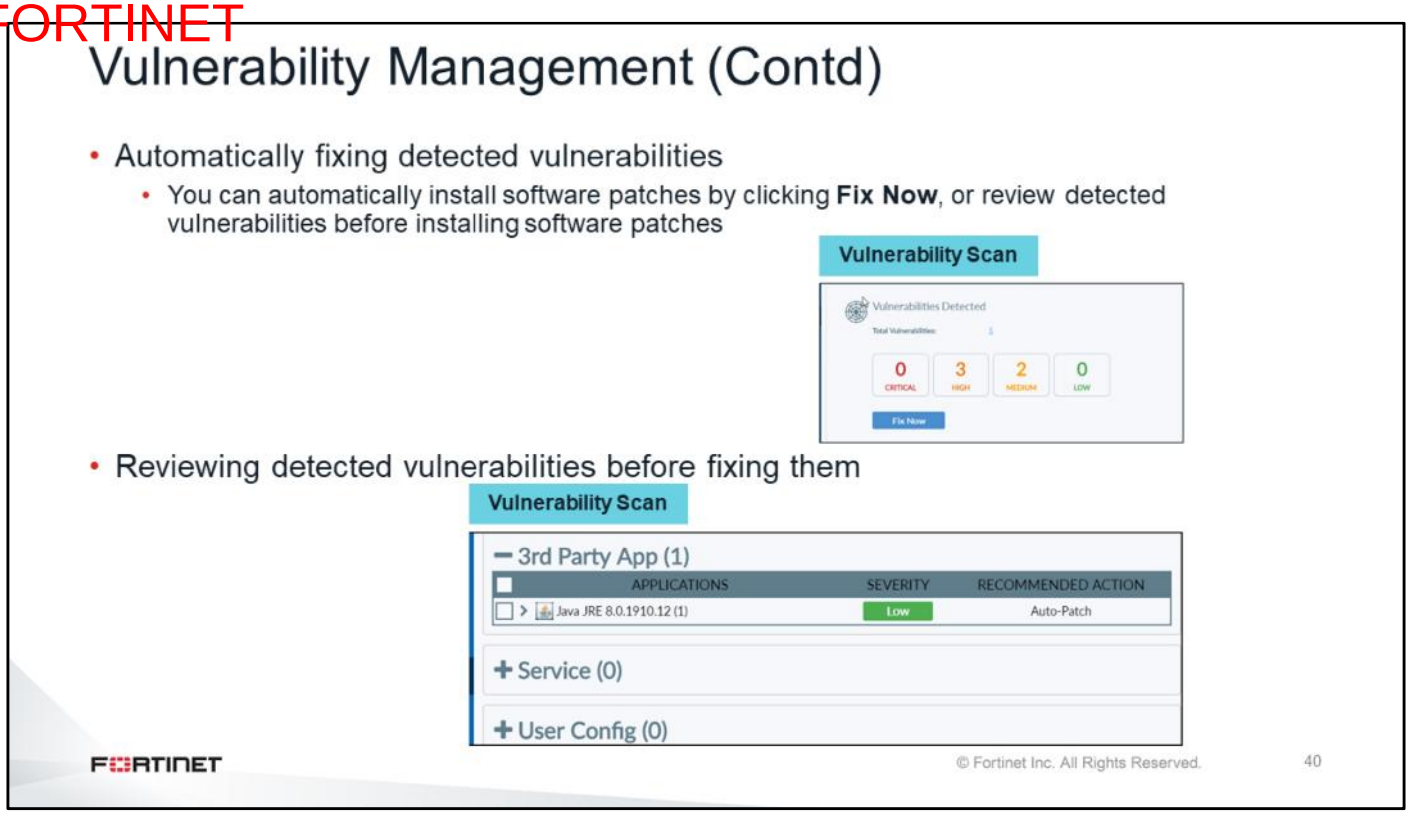
FortiClient communicates with the FortiGuard Center to get the signature updates.

After the scan is complete, FortiClient displays the list of vulnerabilities and details. You can click an item in the list, such as release date, severity, impact, and recommended actions, to name a few.



If compliance is enabled for FortiClient, and EMS compliance rules require it, all automatic and manual software patches must be installed within a time frame that maintains compliant status and network access. The default time frame is one day.

However, the FortiGate administrator may choose a different time frame. Contact your system administrator to learn how long you have to fix vulnerabilities.



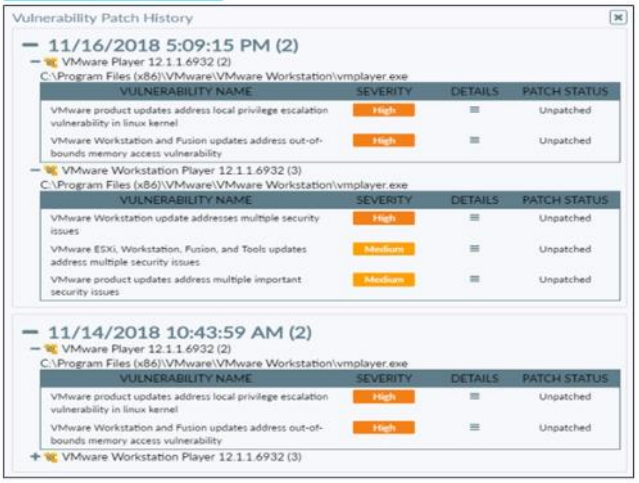
Vulnerability scan identifies vulnerabilities on the endpoint that should be fixed by installing software patches. You can automatically install software patches by clicking **Fix Now**, or you can review detected vulnerabilities before installing software patches. Any software patches that cannot be automatically installed are also listed and you should manually download and install software patches for the vulnerable software.

FortiClient updates vulnerability scan signatures at specific intervals or daily. For intervals, you must select the value in hours, minimum is 1 and the maximum is 24. For daily, you must select a specific time of the day. FortiClient does not support push updates.

Vulnerability Management (Contd)

- Manually fixing detected vulnerabilities
  - In some cases, FortiClient cannot automatically install software patches, and you must manually download and install software patches
- Viewing vulnerability scan history

Vulnerability Scan

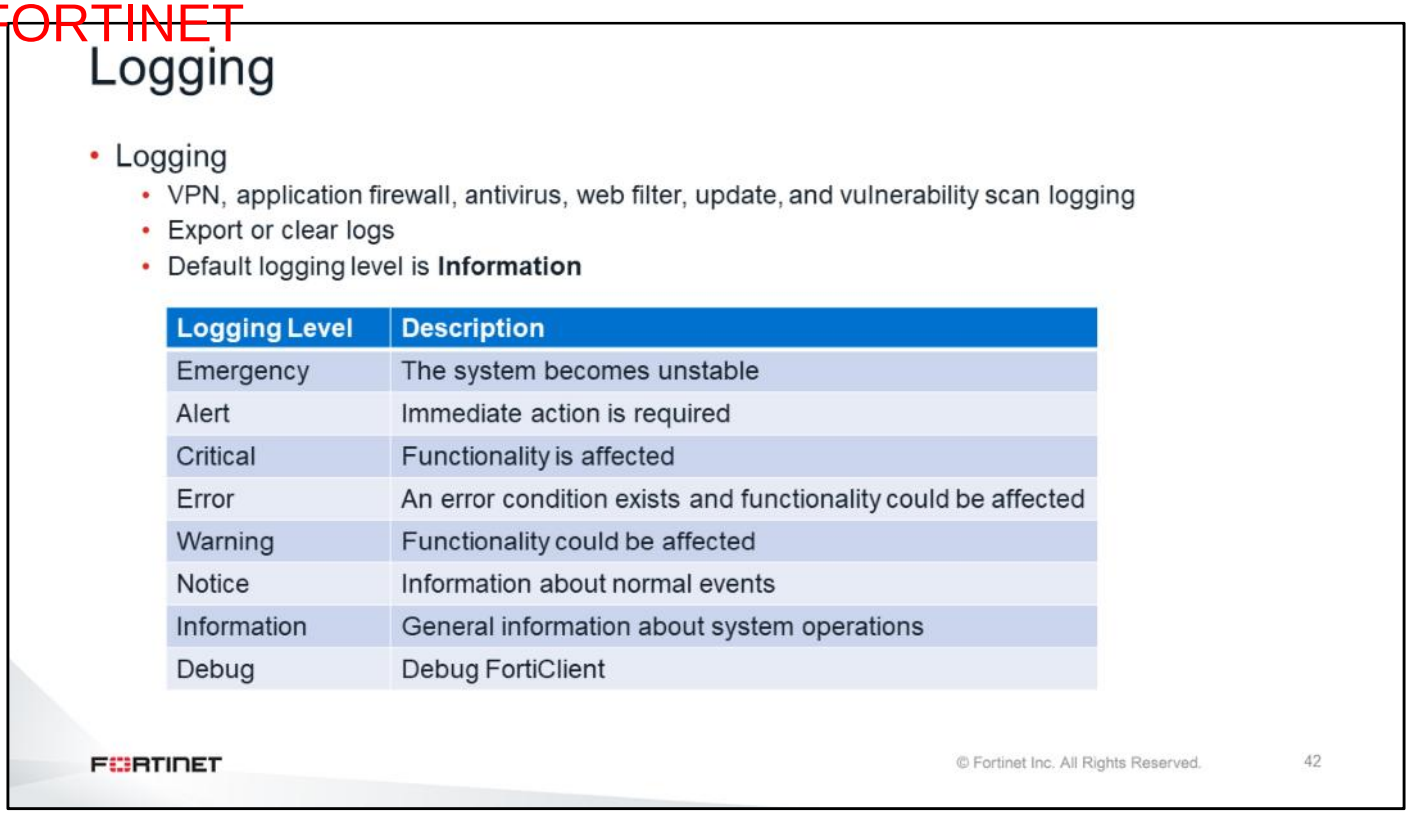


FORTINET

41

When the scan is complete, FortiClient displays a summary of vulnerabilities found on the endpoint. If any detected vulnerabilities require you to manually install remediation patches, the list of affected software is also displayed.

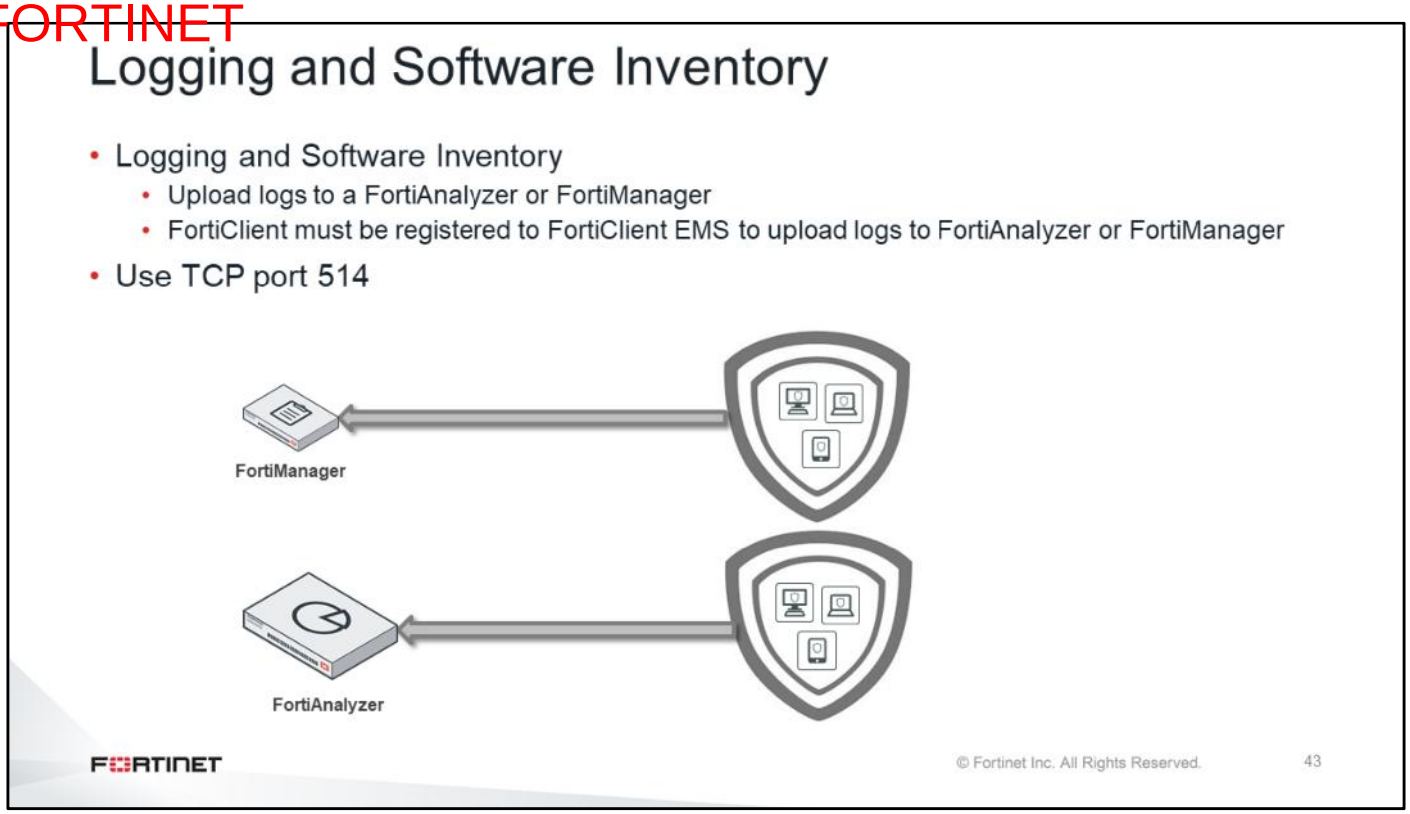
You can view the history of the last seven vulnerability scans and patches. You can view the history to see what software was identified as vulnerable and whether patches for the vulnerabilities were installed.



You can export the log file (.log) from FortiClient.

FortiClient provides options for logging levels, such as information, notice, or emergency. When FortiClient is managed by FortiClient EMS, the administrator can configure the XML configuration to set the logging levels.

The default logging level on FortiClient is **Information**.



FortiClient can be configured to send logs and software inventory reports to FortiAnalyzer or FortiManager. The following products are required:

- FortiClient
- EMS
- FortiAnalyzer or FortiManager

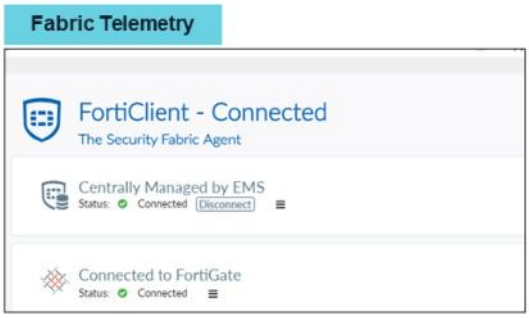
FortiClient uses TCP port 514 to upload to FortiAnalyzer or FortiManager. FortiClient collects information on regular software installed on the endpoint and sends the information to EMS and FortiAnalyzer. FortiClient sends the software inventory information when it first registers on EMS and when it first sends data to FortiAnalyzer. If software changes occur on the endpoint, such as installing new software, updating existing software, or removing existing software, FortiClient sends an updated inventory to EMS and FortiAnalyzer.

FortiClient Telemetry must connect to EMS for FortiClient to upload logs and software inventory reports to FortiAnalyzer or FortiManager.

Note that you must enable logging on FortiManager. By default, this feature is disabled.

Fabric Telemetry—FortiClient Telemetry

- Displays whether FortiClient telemetry is connected to EMS or EMS and FortiGate
- Tab is used to manually connect FortiClient telemetry to EMS and to disconnect
- FortiClient Telemetry
  - FortiClient uses a gateway IP address to connect to FortiGate or EMS
  - FortiClient registers on FortiGate only if the following are true:
    - FortiClient is registered to EMS
    - FortiClient has received a telemetry gateway list from EMS
    - EMS has allocated a Fabric Agent license



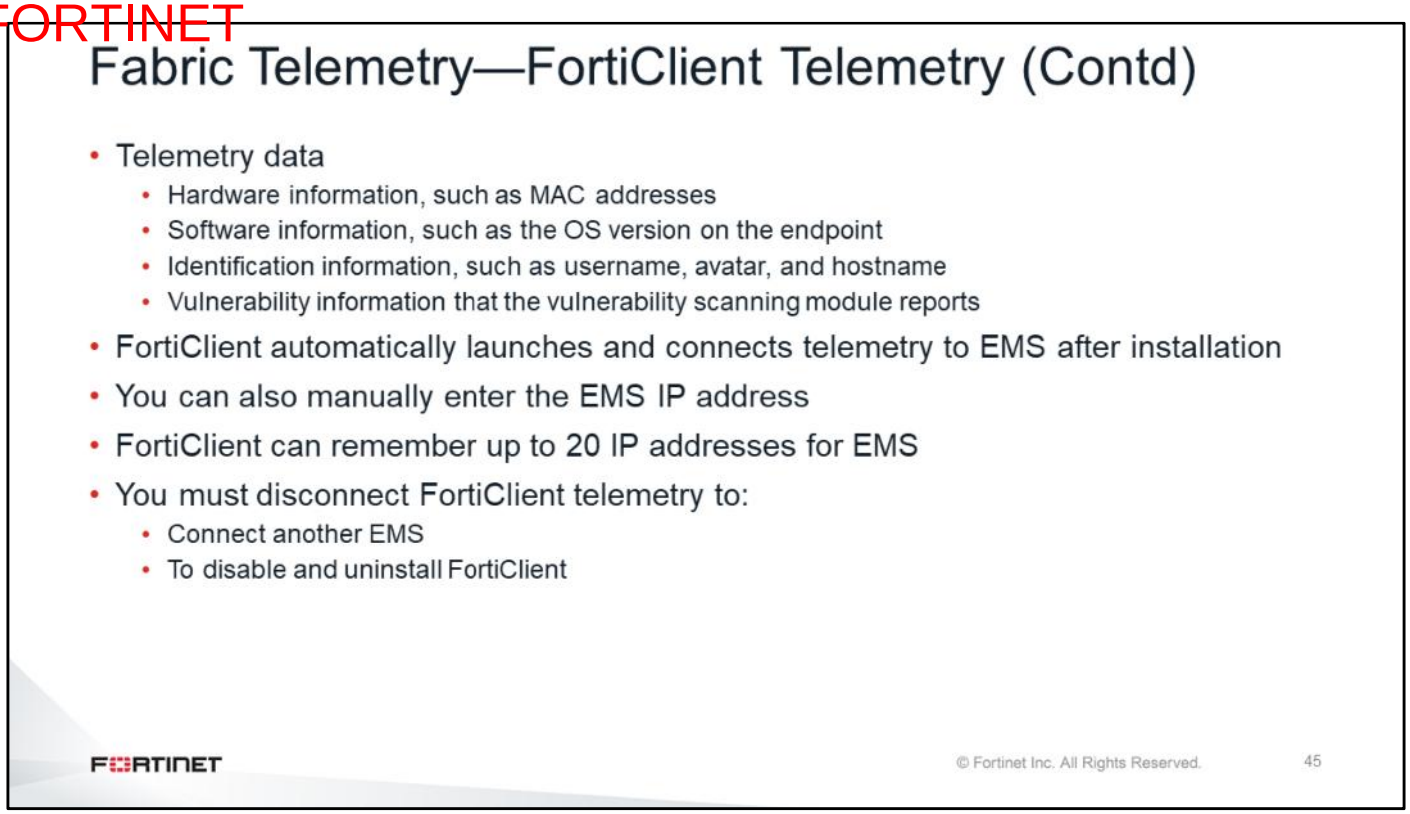
FORTINET

44

The **Fabric Telemetry** tab displays whether FortiClient Telemetry is connected to EMS or EMS and FortiGate. You can use the **Fabric Telemetry** tab to manually connect FortiClient Telemetry to EMS and to disconnect FortiClient Telemetry from EMS.

FortiClient can use a gateway IP address to connect FortiClient Telemetry to FortiGate or EMS. FortiClient only registers to a FortiGate if all of the conditions shown on this slide are true.

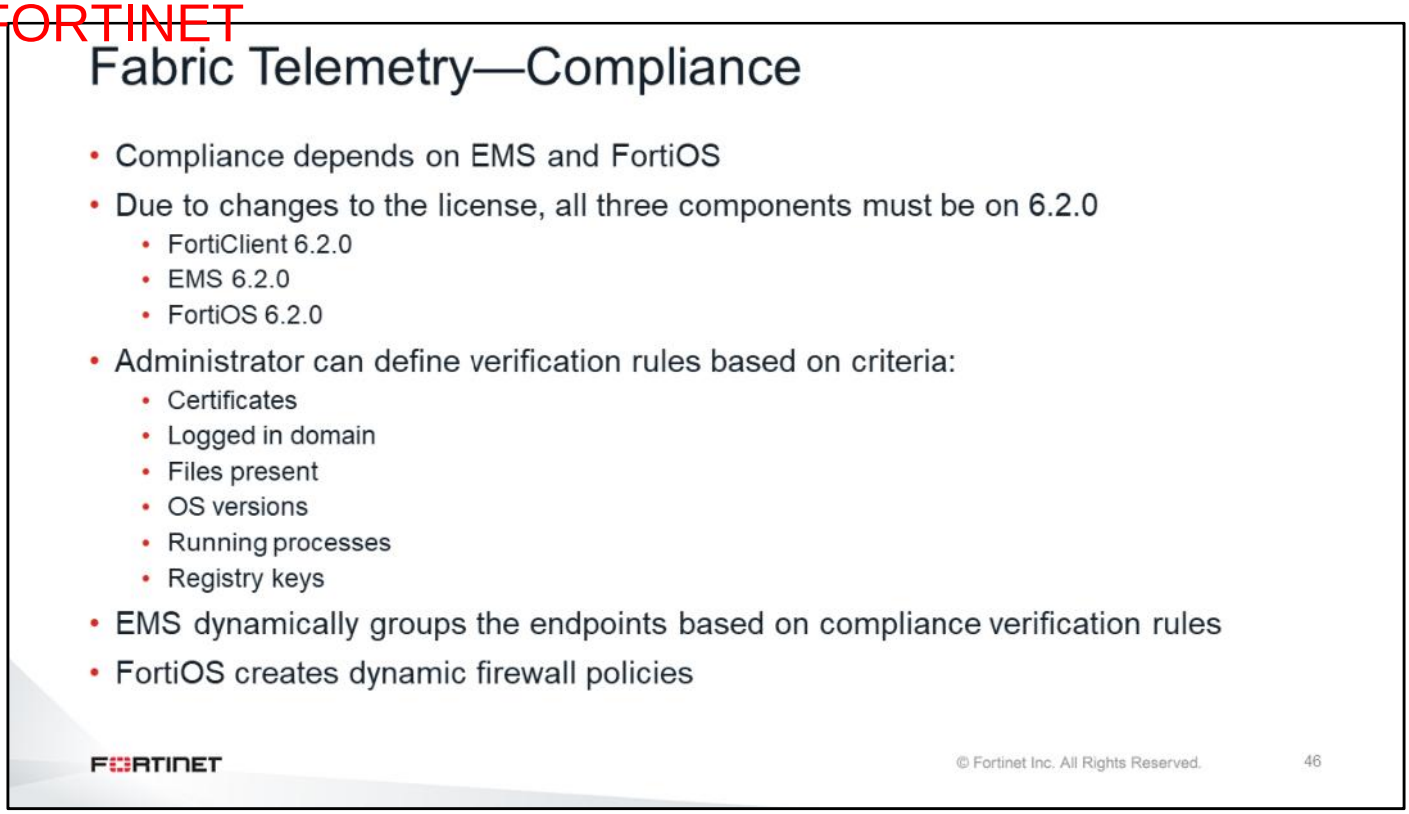
If FortiClient becomes unregistered from EMS, it also becomes unregistered from the FortiGate.



When FortiClient Telemetry is connected to EMS, or EMS and FortiGate, FortiClient collects the hardware information (MAC addresses), software information (OS version on the endpoint), identification information (username, avatar, and hostname), and vulnerability information that the vulnerability scanning module reports about the endpoint, and its workload, and sends it to EMS, or EMS and FortiGate. When FortiClient Telemetry is connected to FortiGate, the Security Fabric uses the information to understand the endpoint and its workload to better protect it.

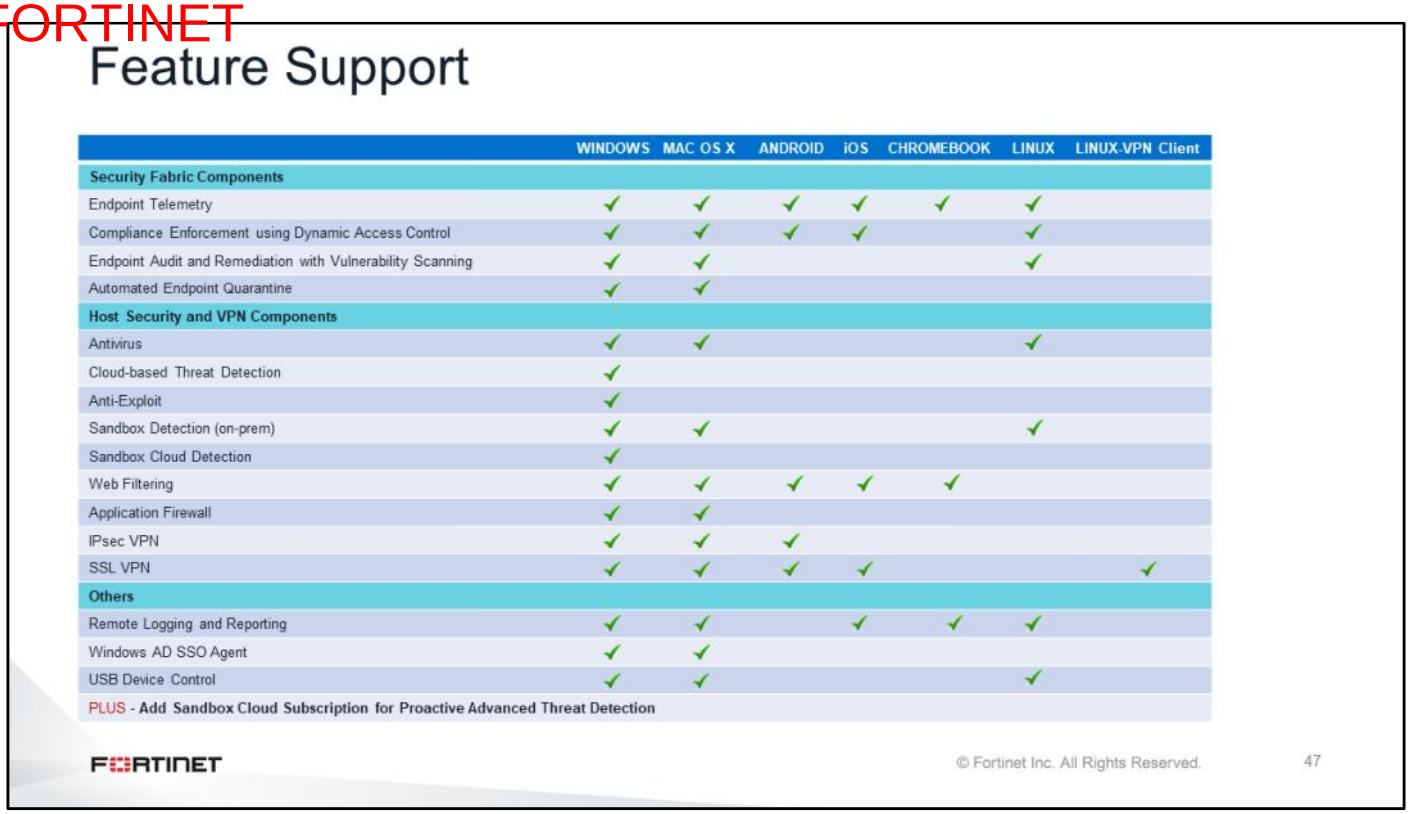
After installation, FortiClient automatically launches and connects telemetry to the EMS server that created the installed deployment package. You can also manually enter the EMS IP address to connect. When you confirm the telemetry connection to EMS, you can instruct FortiClient to remember the EMS IP address. If a connection key is required, FortiClient remembers the connection key too. FortiClient can remember up to 20 IP addresses for EMS.

When you instruct FortiClient to forget an IP address for EMS, FortiClient Telemetry does not use the IP address to automatically connect to EMS when re-joining the network. You must disconnect FortiClient Telemetry from EMS to connect to another EMS or to disable and uninstall FortiClient.



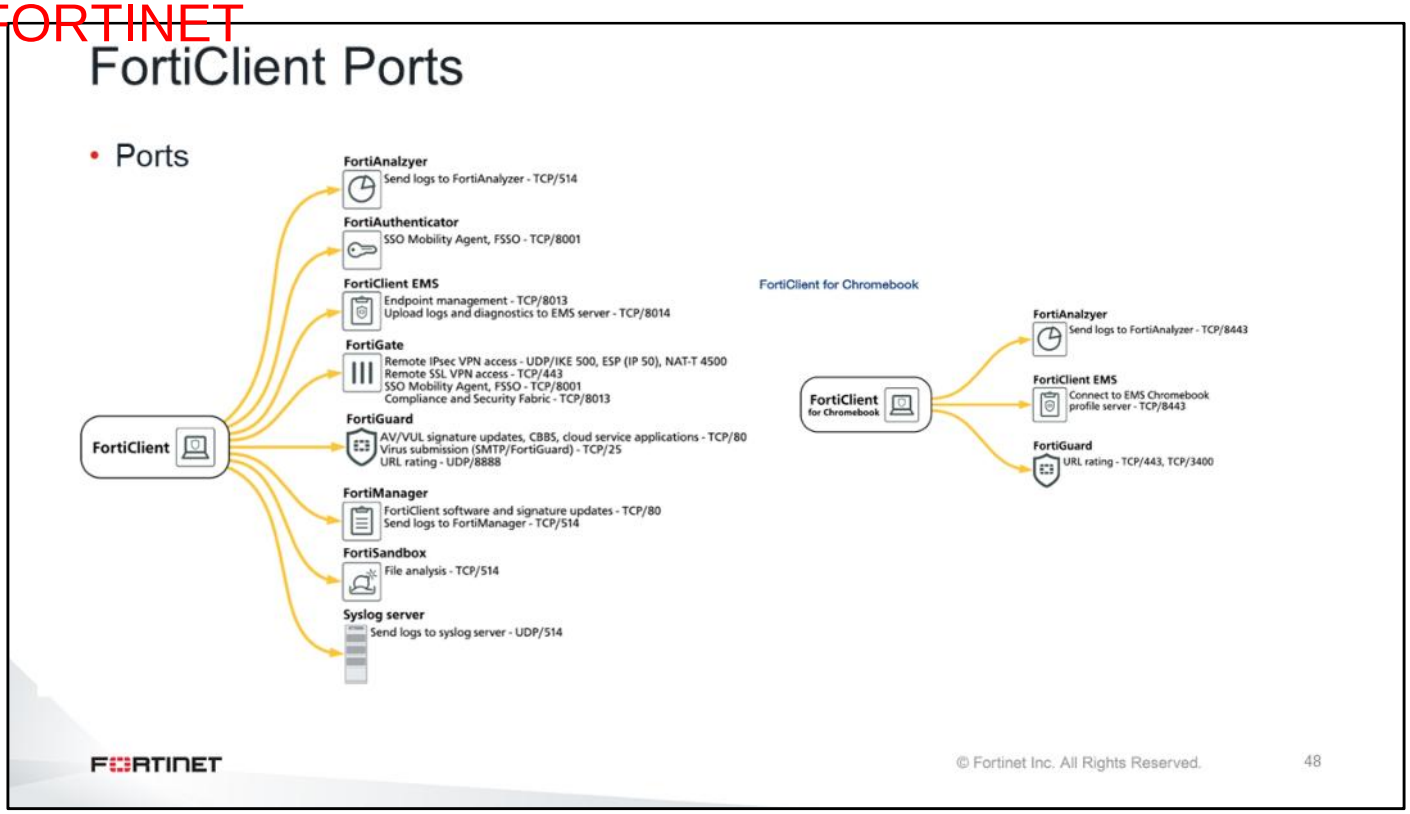
In FortiClient 6.2.0, compliance depends on EMS and FortiOS. This feature is only available if using FortiClient 6.2.0 with EMS 6.2.0 and FortiOS 6.2.0. Due to changes to the license we can't have a mixed version environment.

The administrator can define compliance verification rules on EMS based on criteria, such as certificates, the logged in domain, files present, OS versions, running processes, and registry keys. When a FortiClient endpoint registers on EMS, EMS dynamically groups the endpoint based on the compliance verification rules. FortiOS can receive the dynamic endpoint groups from EMS and use them to create dynamic firewall policies. The endpoint may be unable to access the network based on the compliance verification rules.



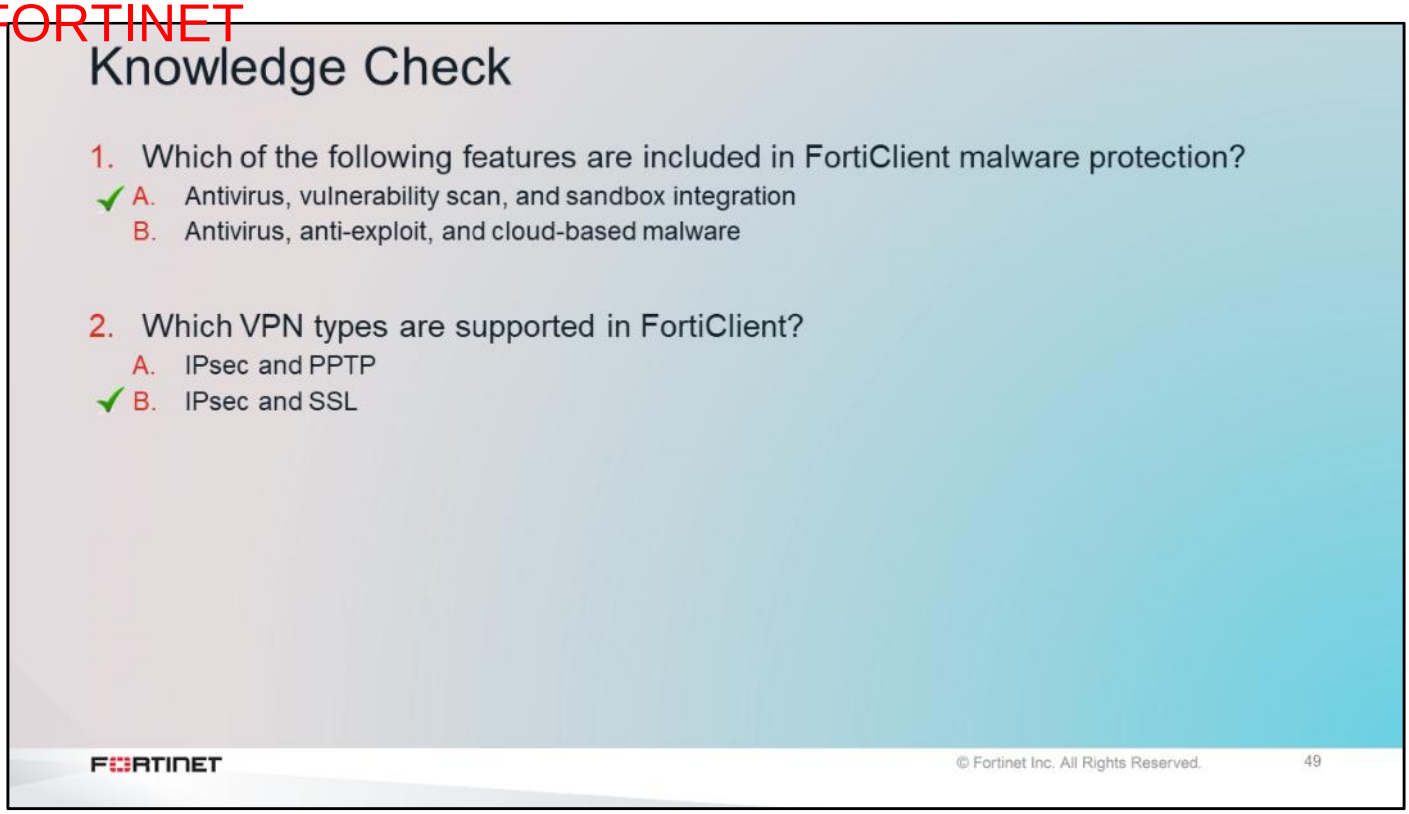
FortiClient 6.2.0 supports a number of features, such as VPNs, antivirus, web filtering, and more. When FortiClient is registered with FortiGate or FortiClient EMS, it enhances comprehensive security, helping you to safeguard your systems with advanced security technologies, which are all managed from a single management console with easy provisioning, monitoring, and auditing.

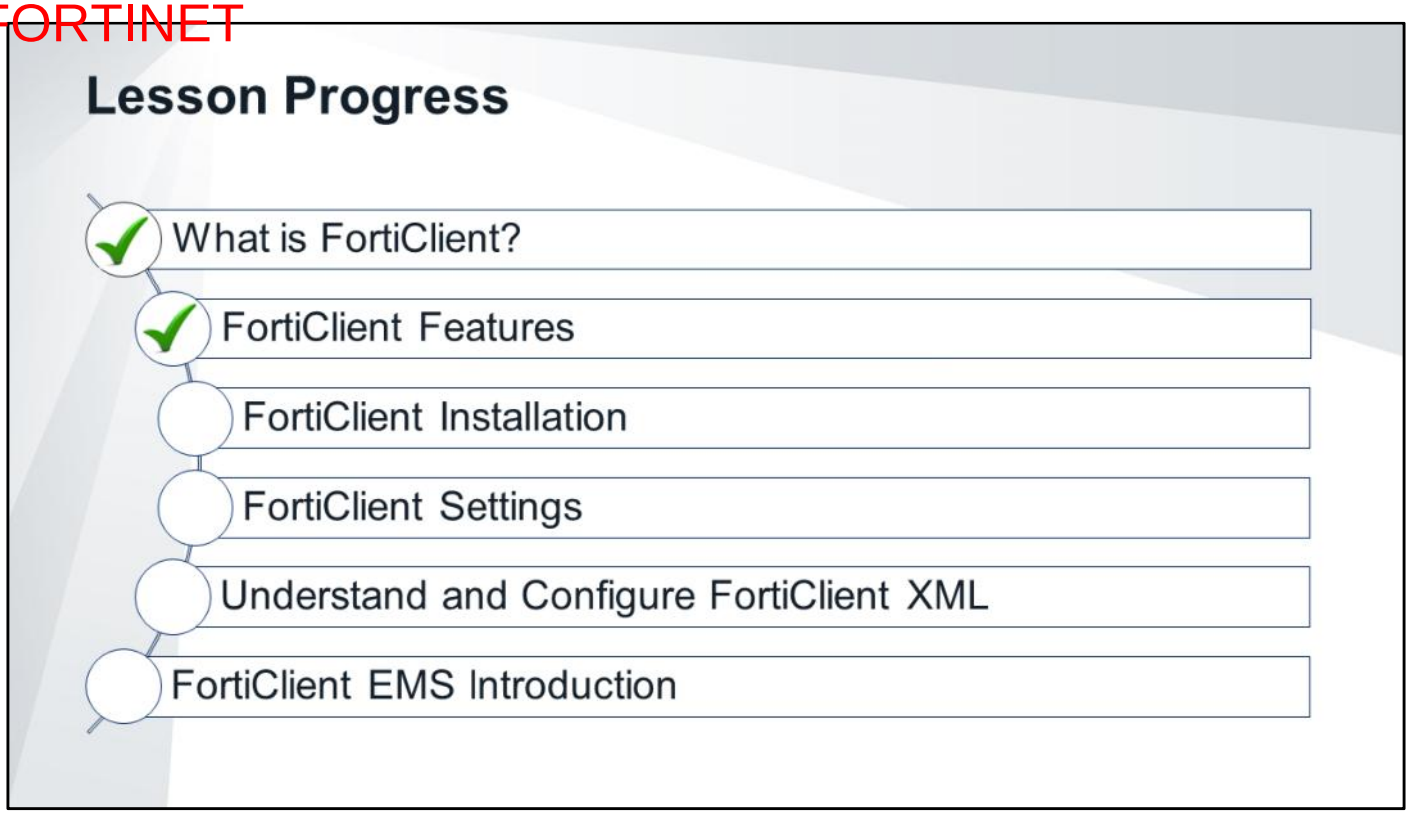
You can also customize the FortiClient installation and use VPN auto-connect to ensure that FortiClient creates a VPN connection to the FortiGate when it is considered to be off-net. FortiClient also supports configuration provisioning for iOS (.mobileconfig files) in addition to FortiClient configuration provisioning.



You use FortiClient ports to communicate with other Fortinet products.

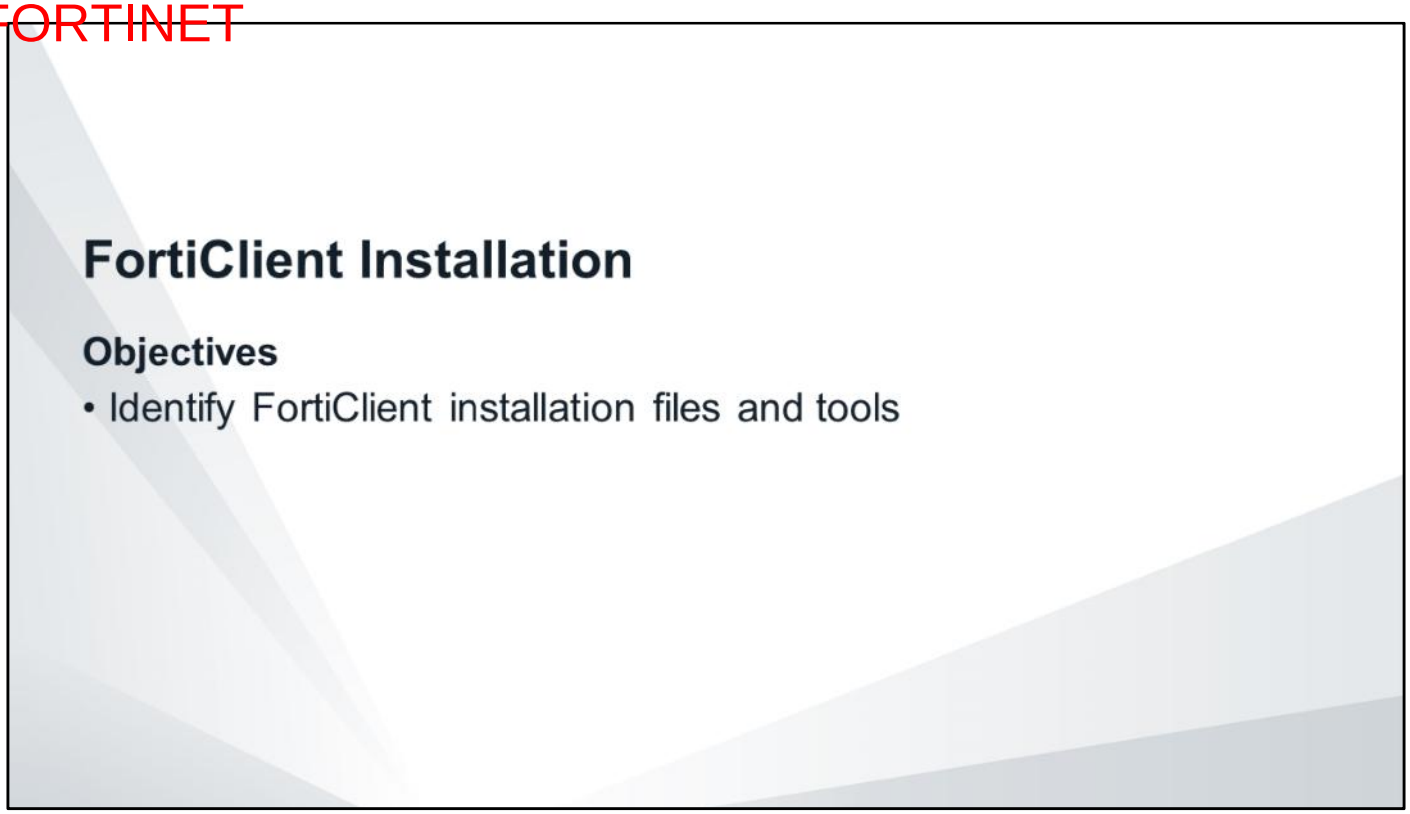
Note that Chromebook port TCP 3400 for URL rating is only used with EMS.





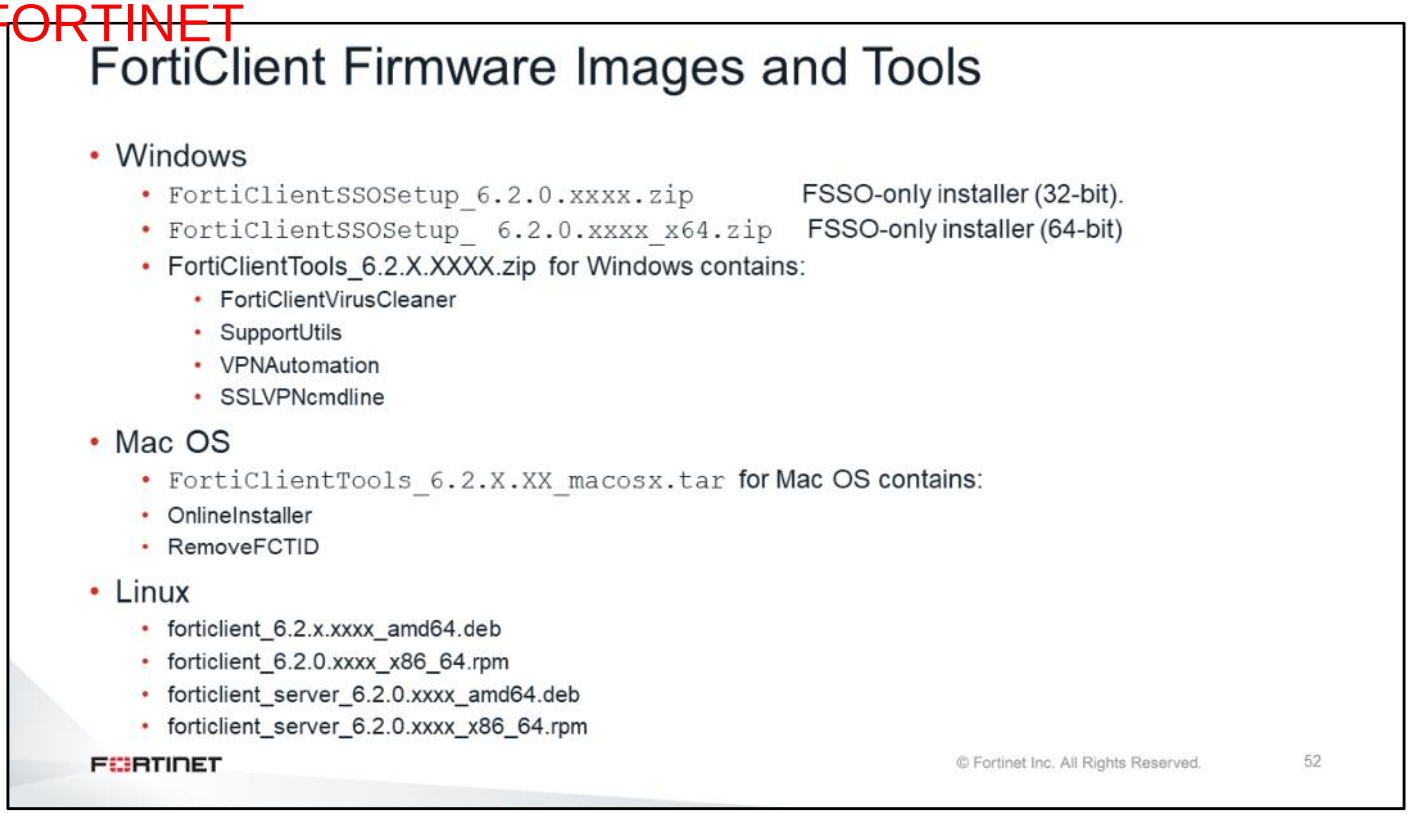
Good job! You now know FortiClient features.

Now, you will learn about FortiClient installation options.



After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in identifying and understanding FortiClient installation options, tools, and features, you will be able to select the appropriate options and tools to install FortiClient in your network.



The files mentioned are available in the firmware image file folder on the Fortinet Support Portal.

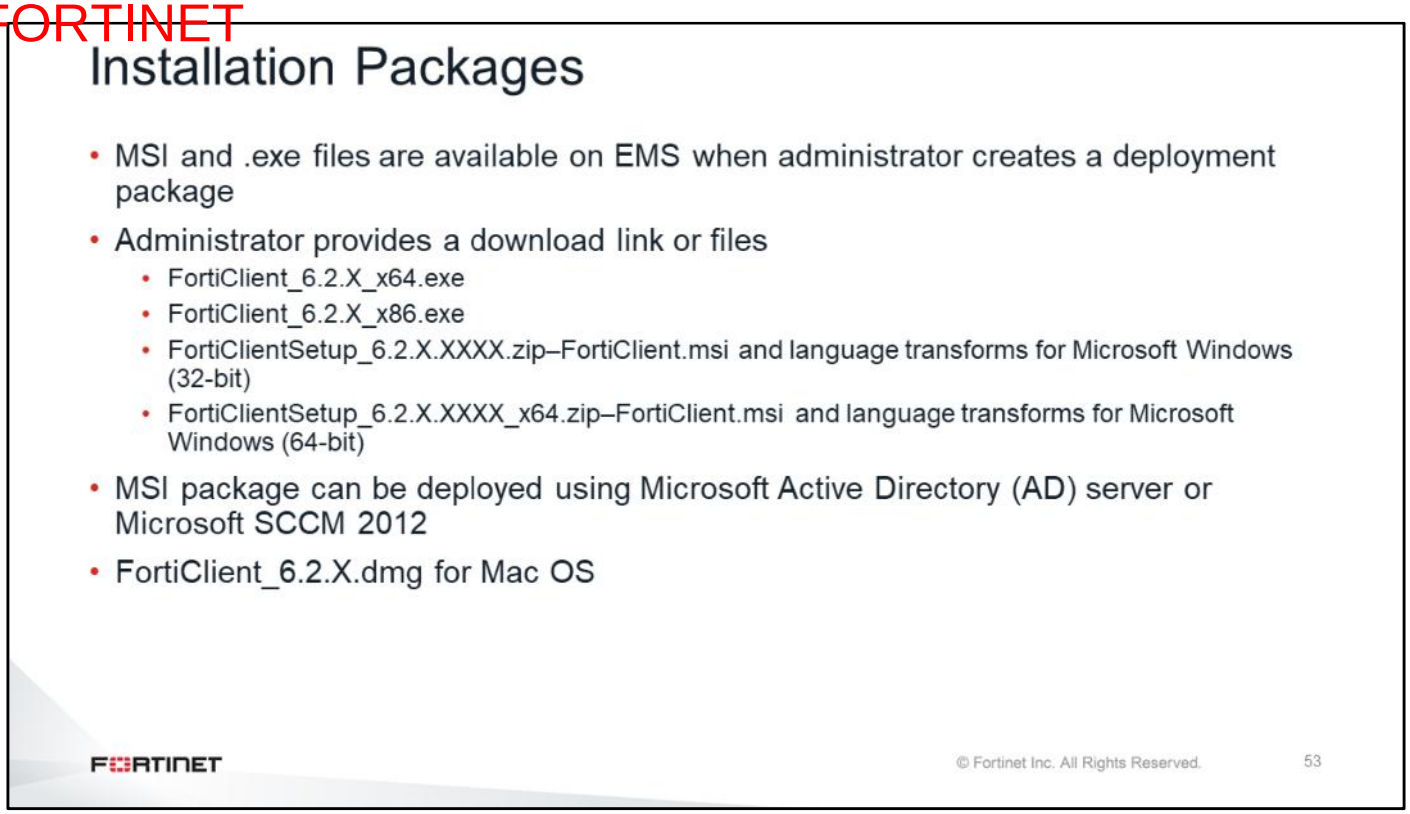
The FortiClient tools package contains various tools you can use to customize your FortiClient installation. The FortiClientVirusCleaner tool was developed to identify and cleanse systems of viruses.

SupportUtils folder contains various tools:
- **RemoveFCTID.exe**: A tool to remove the unique identifier
- **FCRemove.exe**: A cleanup tool for use only if the **Add/Remove Programs** applet fails to remove FortiClient
- **ReinstallNIC.exe**: A tool for use on Windows 7 if DHCP address allocation is slow
- **FortiClient_Diagnostic_Tool.exe**: A tool to gather information, such as the FortiClient connection to FortiGuard Distribution Server (FDS), general system information, and installed feature information, all of which can be useful for troubleshooting

VPNAutomation includes `FCCOMIntDLL.tlb`, which is a type of library needed for building applications that use the FortiClient IPsec VPN COM interface, and SSLVPNcmdline includes `FortiSSLVPNClient.exe`, which is a command line tool for controlling SSL-VPN tunnels.

The Mac OS X FortiClient tools file contains an online installer which downloads and installs the latest FortiClient file from the public FDS, and `RemoveFCTID.exe` to remove the unique identifier.

For files in the Linux folder, refer to this slide.



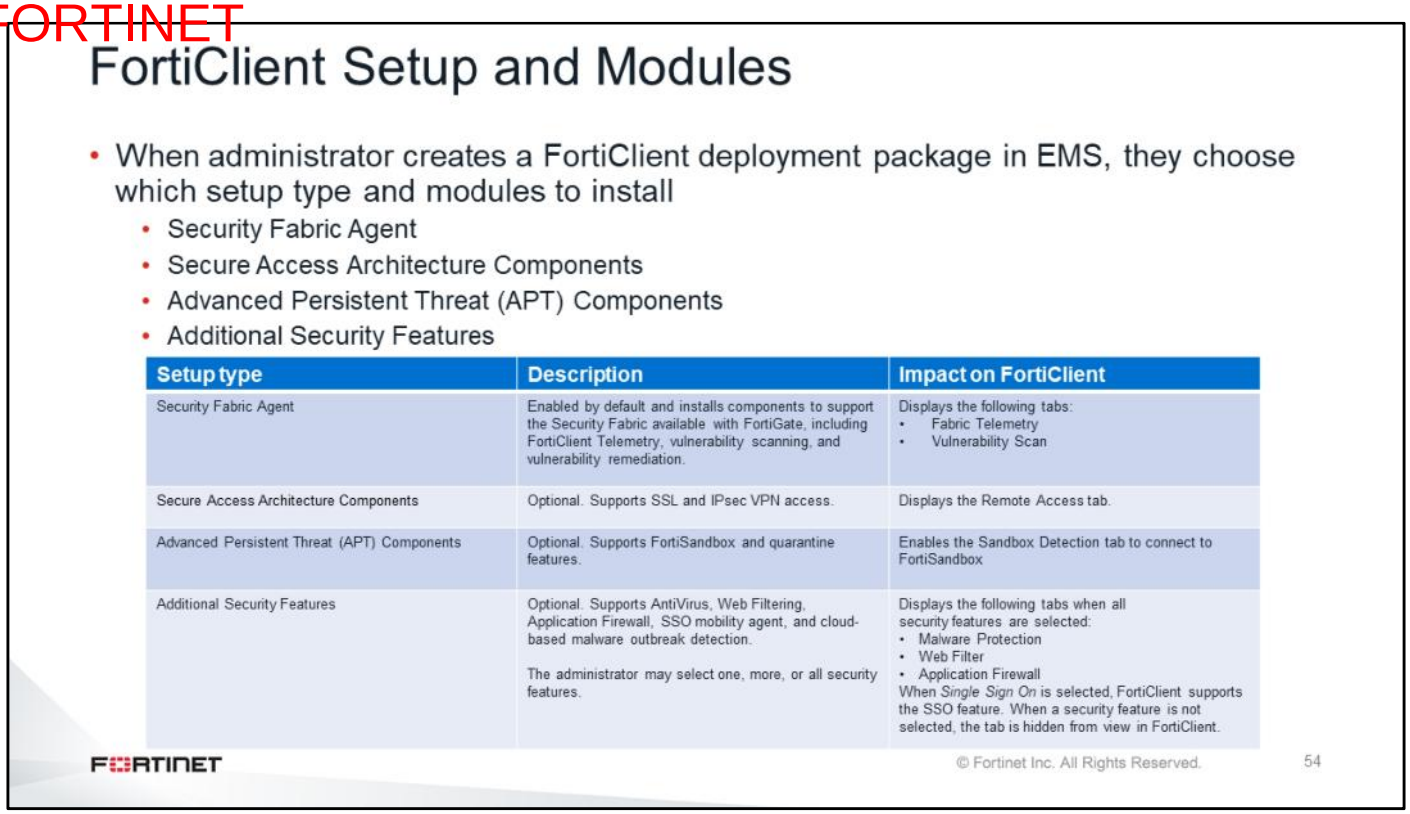
In 6.2.0, The FortiClient (Windows) installer is available on EMS. You can configure and select installed features and options on EMS. The administrator configures a FortiClient deployment package in EMS that includes an .exe and MSI file. The administrator specifies which modules to install in the deployment package. The EMS administrator will provide a download link to the FortiClient installation files.

MSI installers are supported in Microsoft Windows environments only.

`FortiClientSetup_6.2.X.zip`: A zip package containing FortiClient.msi and language transforms for 32-bit Windows. Some properties of the MSI package can be customized with a custom installer.

`FortiClientSetup_6.2.X_x64.zip`: A zip package containing FortiClient.msi and language transforms for 64-bit Windows. Some properties of the MSI package can be customized with a custom installer.

The MSI installer in the .zip file package is customizable for a larger rollout to many computers in an organization.

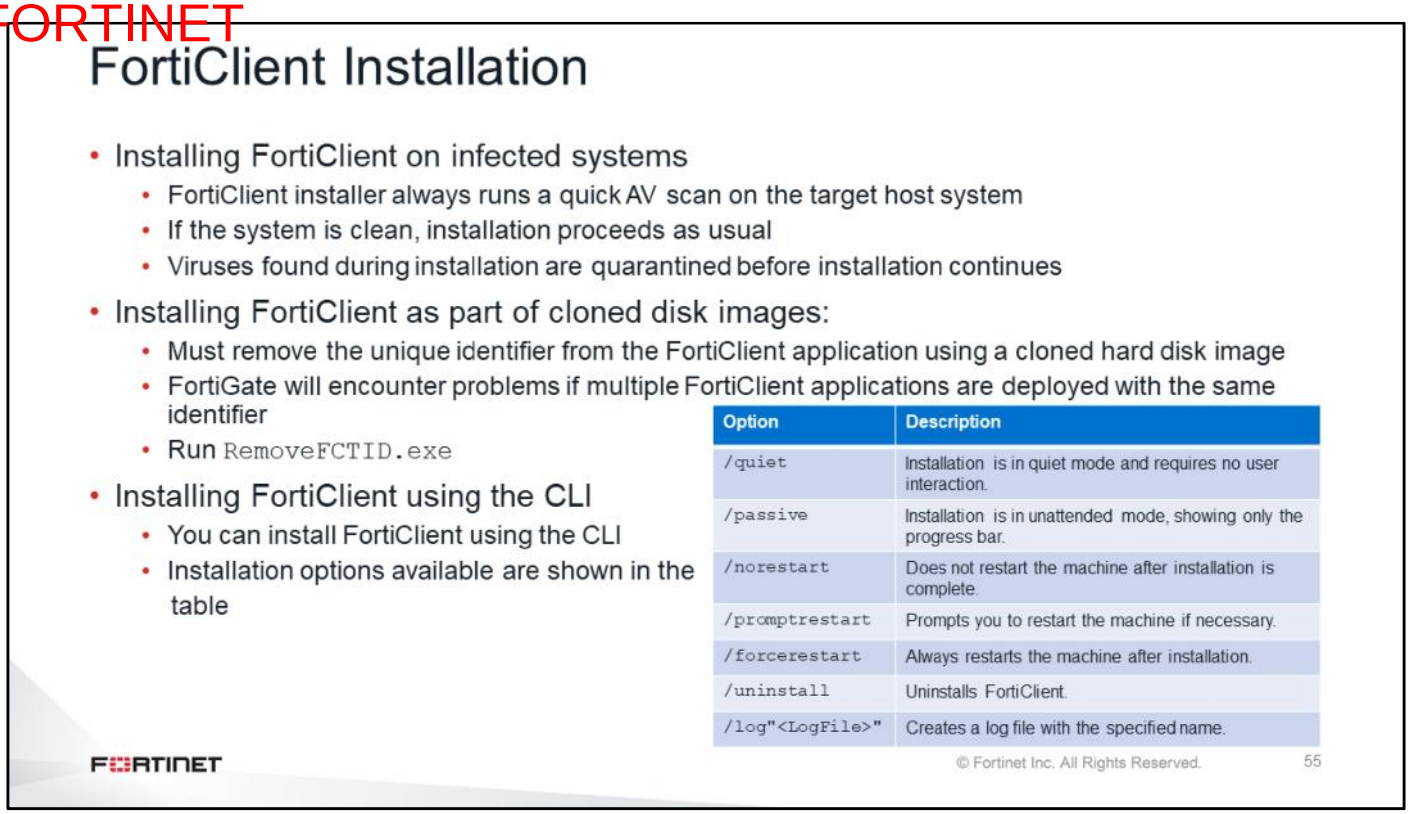


When the administrator creates a FortiClient deployment package in EMS, they choose which setup type and modules to install:

- Security Fabric Agent
- Secure Access Architecture Components
- Advanced Persistent Threat (APT) Components
- Additional Security Features

The impact of the options are shown on this slide. The administrator can use an EMS profile to disable installed components on FortiClient but cannot use an EMS profile to enable uninstalled components on FortiClient.

For example, if the administrator creates the EMS installer with APT components selected, the **Sandbox Detection** tab is enabled on FortiClient. The administrator can use an EMS profile to disable **Sandbox Detection**. However, if the installer did not include APT components, the **Sandbox Detection** tab is disabled on FortiClient and the administrator cannot use an EMS profile to enable **Sandbox Detection**.



The FortiClient installer always runs a quick AV scan on the target host system before proceeding with the complete installation. If the system is clean, installation proceeds as normal. Any virus found during this step is quarantined before installation continues. In case a virus on an infected system prevents you from downloading the new FortiClient package, use the following process:

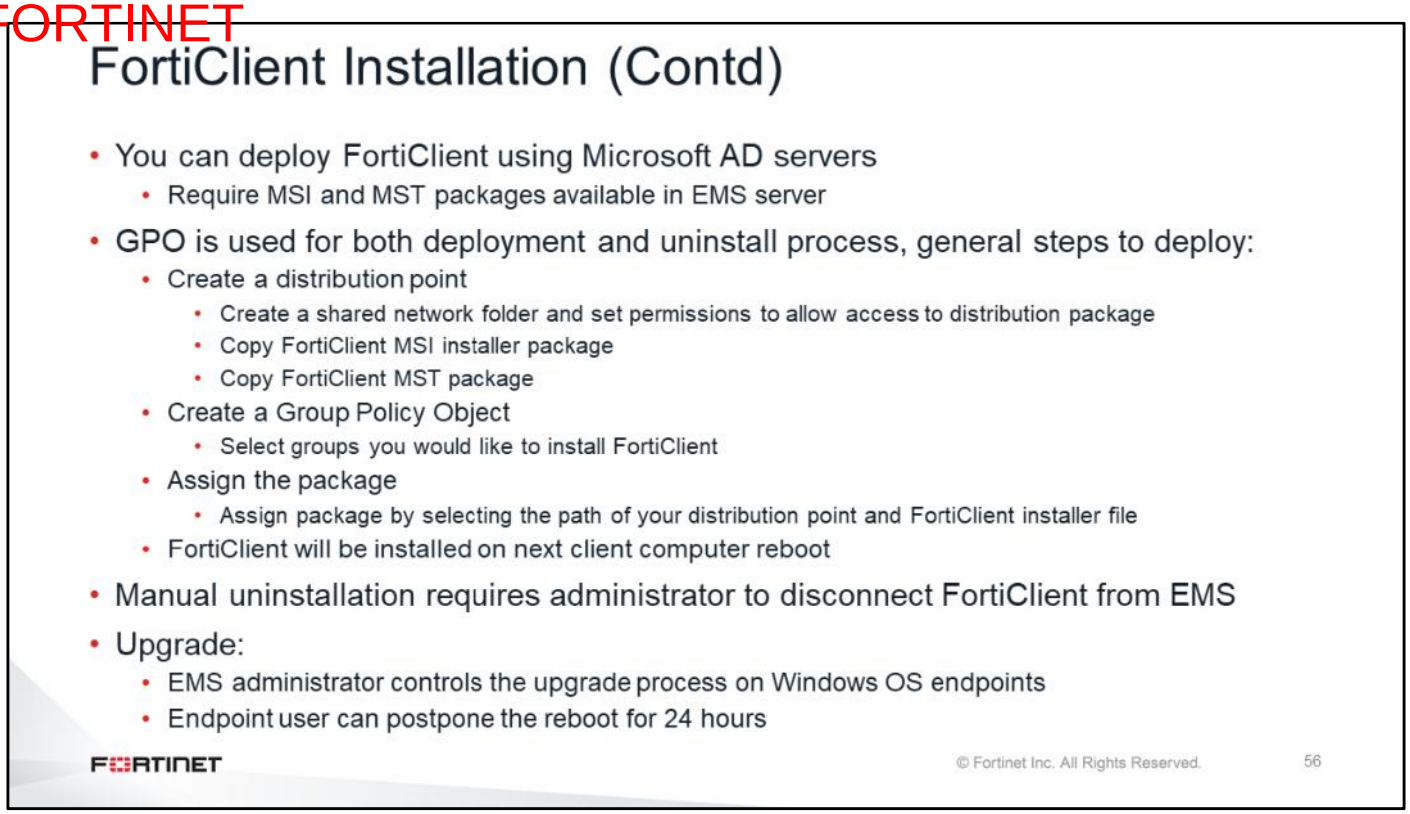
1. Boot into “safe mode with networking”. This is required for the FortiClient installer to download the latest signature packages from the Fortinet Distribution Network.
2. Run the FortiClient installer.

This scans the entire file system. If a virus is found, it is quarantined. When complete, reboot into normal mode and run the FortiClient installer to complete the installation (because Windows does not allow FortiClient installation to complete in safe mode).

If you configure computers using a cloned hard disk image, you must remove the unique identifier from the FortiClient application. You will encounter problems with the FortiGate if you deploy multiple FortiClient applications with the same identifier. You must use the following steps:

1. Install the FortiClient application.
2. Right-click the FortiClient icon in the system tray, and select **Shutdown FortiClient**.
3. From the folder where you expanded the `FortiClientTools.zip` file, run `RemoveFCTID.exe`. The RemoveFCTID tool requires administrative rights. Do not include the RemoveFCTID tool as part of a logon script.
4. Shut down the computer. Do not reboot the Windows operating system on the computer before you create the hard disk image. The FortiClient identifier is created before you log in.
5. Create the hard disk image and deploy it, as needed.

You can also install FortiClient using the CLI. The table in this slide summarizes the installation options available when using the CLI. `FortiClientSetup_6.2.0.1131_x64.exe /quiet /log"Log"` installs FortiClient 6.2.0 build 1131 in quiet mode, creating a log file with the name "Log" .

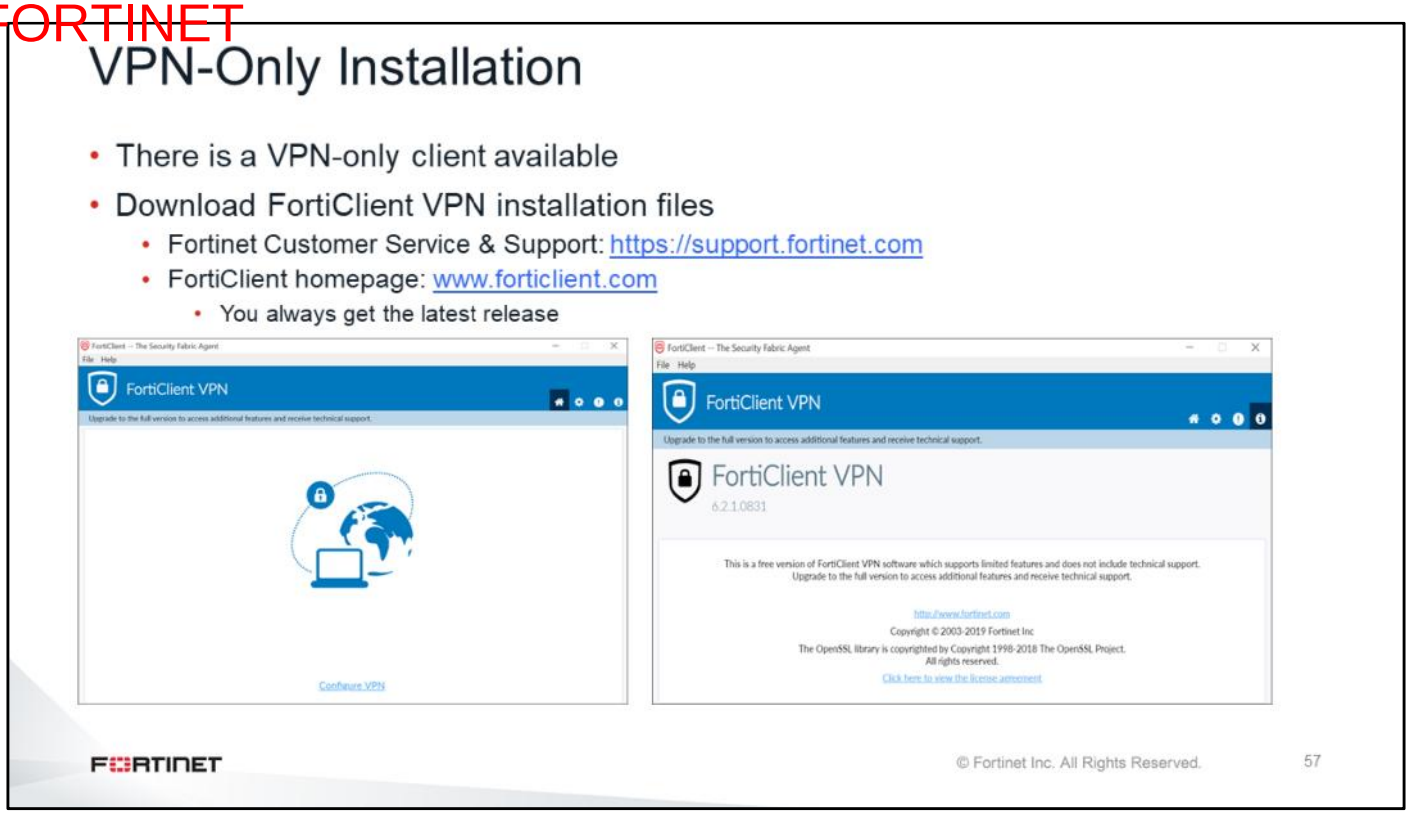


You can deploy FortiClient installation using Microsoft AD servers. On your domain controller, create a distribution point and a shared network folder to distribute the FortiClient MSI installer file available from EMS. Set file permissions on the shared folder to allow access to the distribution package. Now copy the FortiClient MSI installer and MST package into this shared folder.

In your domain, add a new organizational unit (OU) and move all the computers you want to distribute the FortiClient software to, into the newly-created OU. Create a group policy object (GPO), and then create the FortiClient installer package. Force a GPO update. The software is installed on the next reboot of the client computer. You can also wait for the client computer to poll the domain controller for GPO changes and install the software then.

To uninstall FortiClient, you can either use a GPO or manual process. For manual uninstall, disconnect FortiClient from EMS. The endpoint is no longer managed by EMS. Click **Unlock** to unlock the configuration and then shut down FortiClient. Once FortiClient is shut down, uninstall FortiClient using the Windows Add/Remove Programs application.

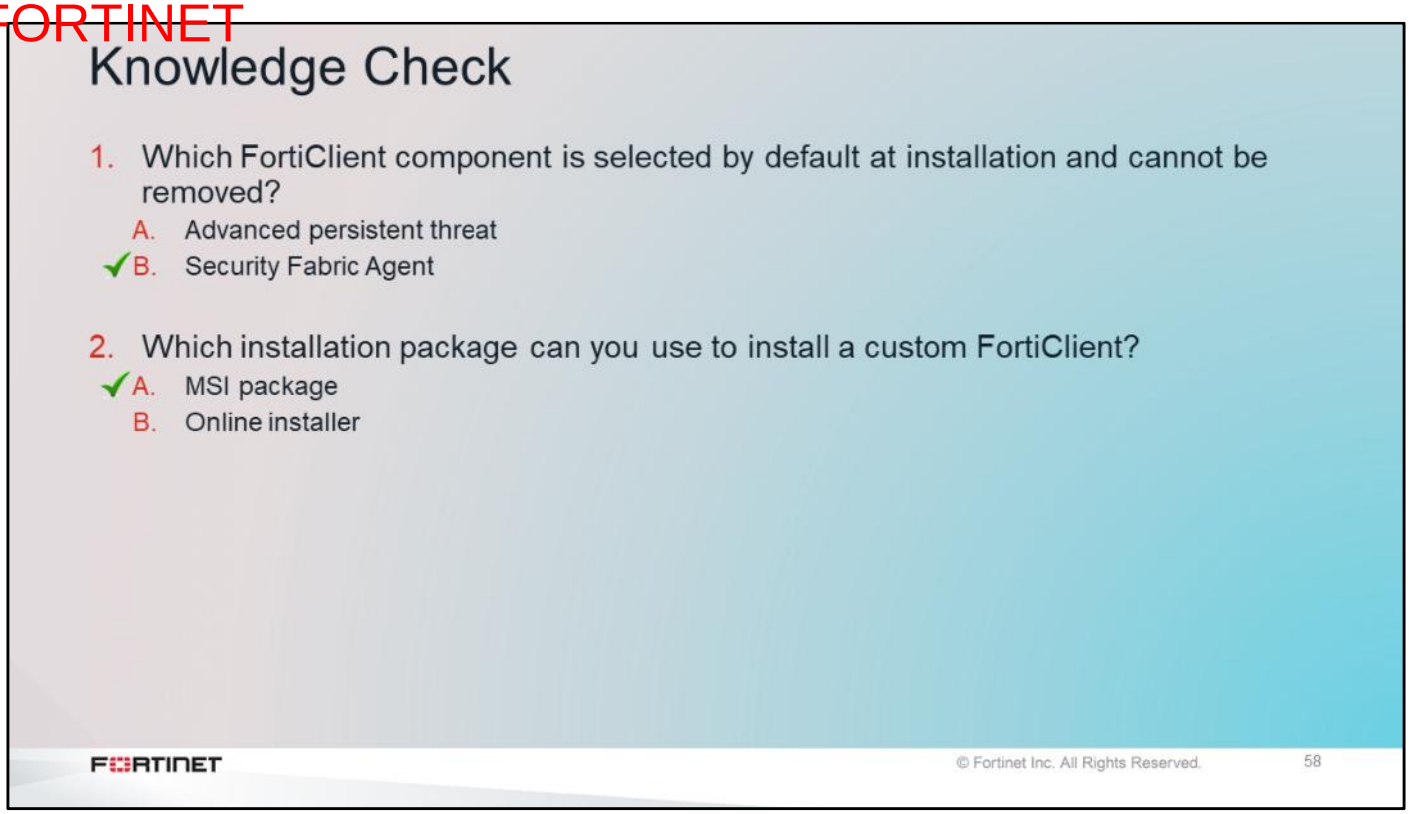
An administrator will control FortiClient upgrades for you. When an administrator deploys a FortiClient upgrade from EMS to endpoints running a Windows operating system, an *Upgrade Schedule* dialog displays in advance on the endpoint to let endpoint users schedule the upgrade and mandatory endpoint reboot. If FortiClient is not installed on the endpoint, a reboot is not required for the installation, and the *Upgrade Schedule* dialog is not displayed. The endpoint user can postpone the reboot for a maximum of 24 hours. Before the mandatory reboot occurs, a FortiClient dialog displays with a 15 minute warning.

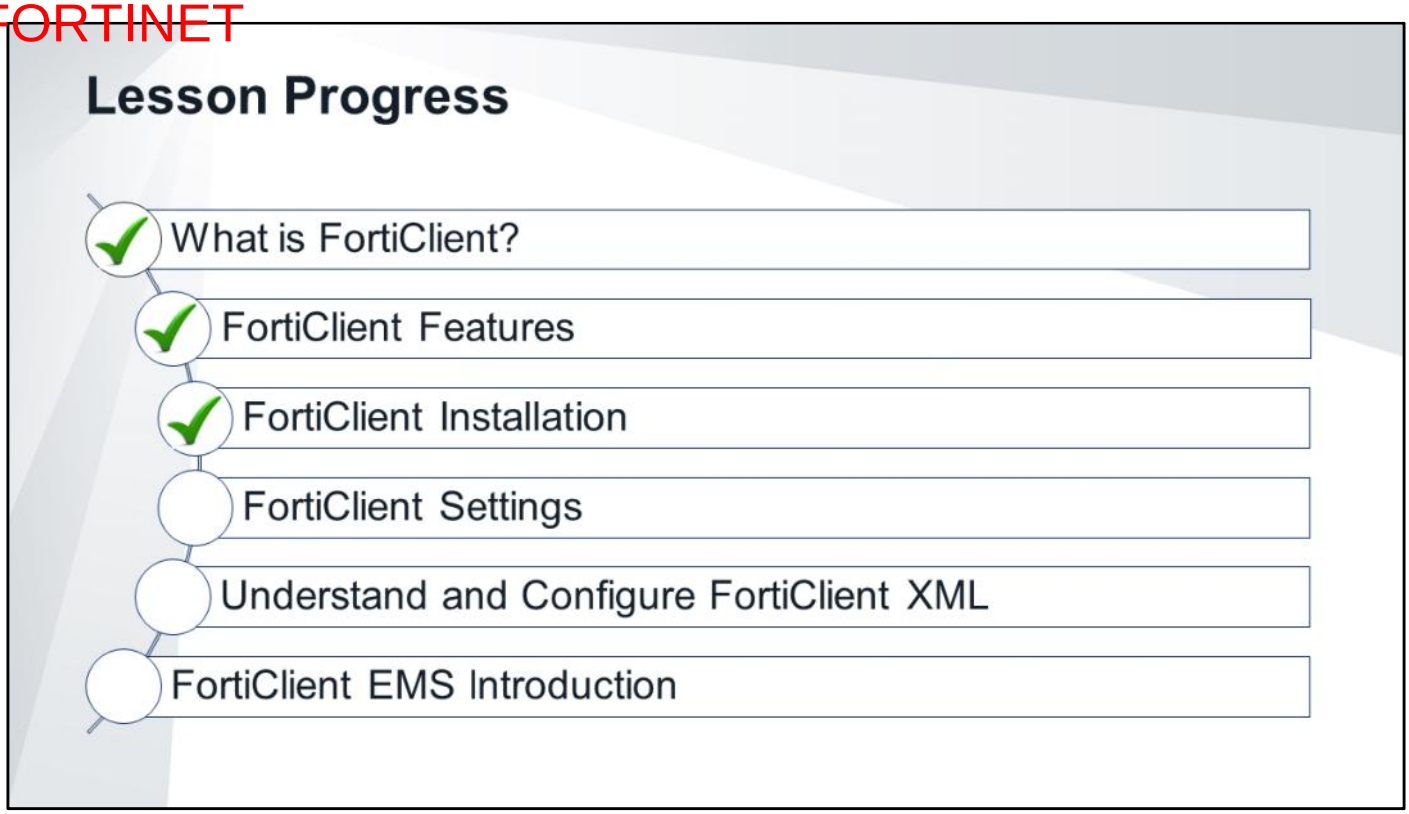


FortiClient 6.2.1 offers a free VPN-only version that you can use for VPN-only connectivity to FortiGate. You can download the VPN-only application from FortiClient.com only. You cannot use the VPN-only client with the FortiClient Single Sign-On Mobility Agent (SSOMA). To use VPN and SSOMA together, you must purchase an EMS license.

On the Fortinet Support website:
- The Windows FortiClient Tools folder includes `FortiClientVPNOnlineInstaller_6.2.exe`, `FortiClientInstaller.exe`, and `FortiClientVPNInstaller.exe`.
- The Mac FortiClient Tools folder includes `FortiClientVPNOnlineInstaller_6.2.dmg, and FortiClient_6.2.X.XXX_Installer.dmg`.

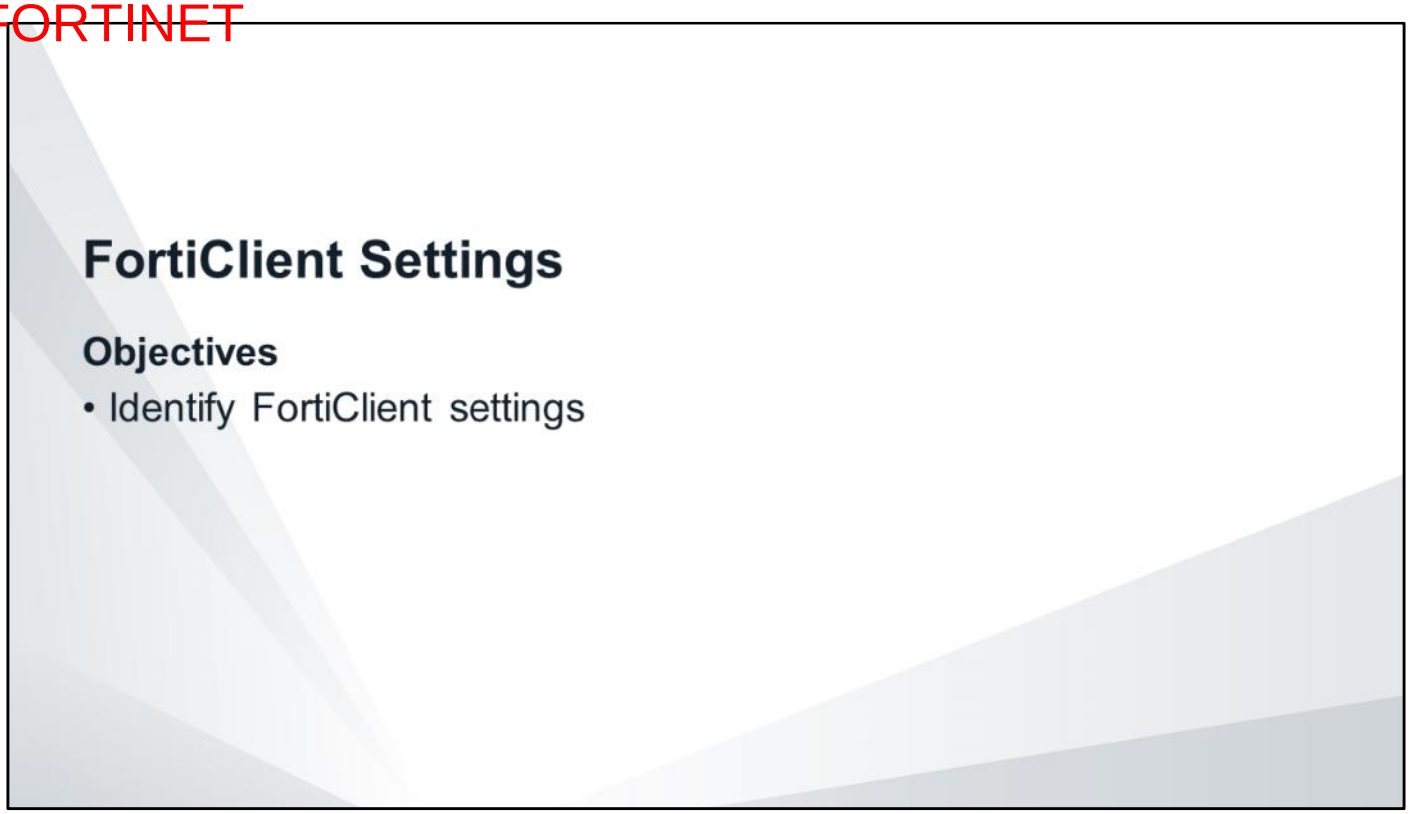
If FortiClient does not register on EMS or obtain a valid Fabric Agent license during the three-day free VPN access, the Remote Access feature becomes unavailable. At this point, the endpoint must be able to reach EMS without a VPN connection to connect to EMS. Upon successfully receiving a license from EMS, EMS enables all FortiClient features configured on the assigned endpoint profile.





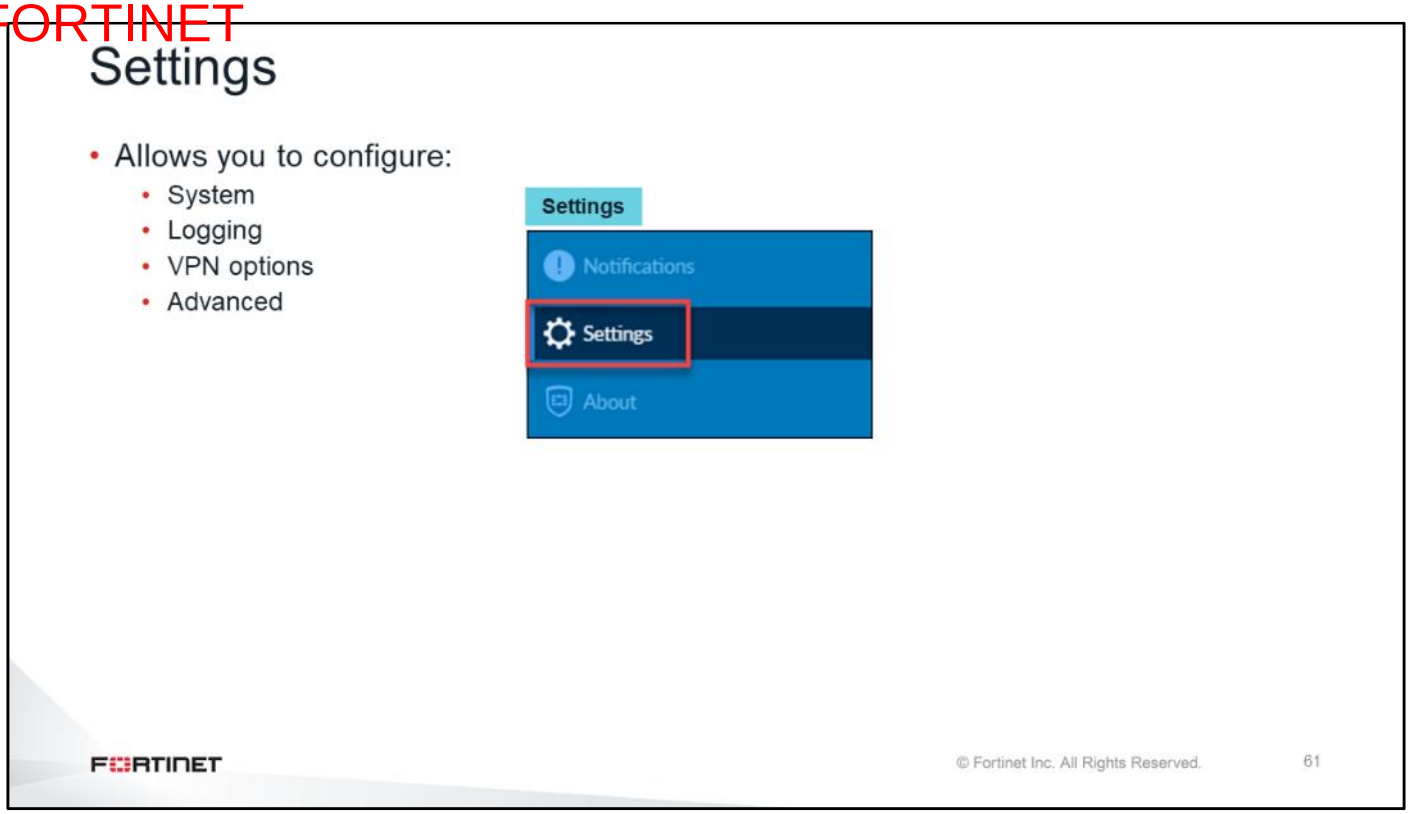
Good job! You now know how to install FortiClient.

Now, you will learn about FortiClient general settings.



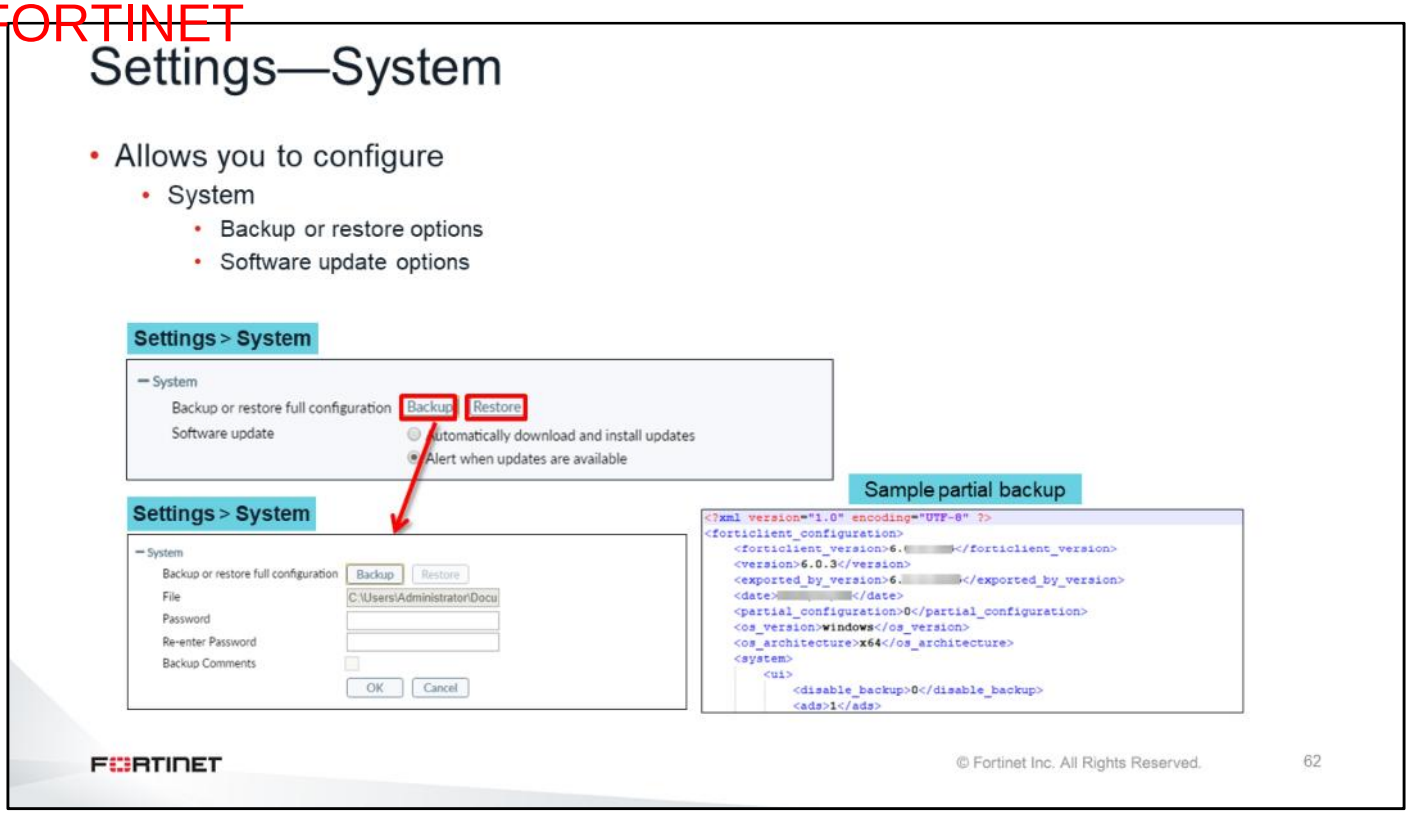
After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence in understanding FortiClient settings, you will be able to use them effectively when setting up FortiClient.



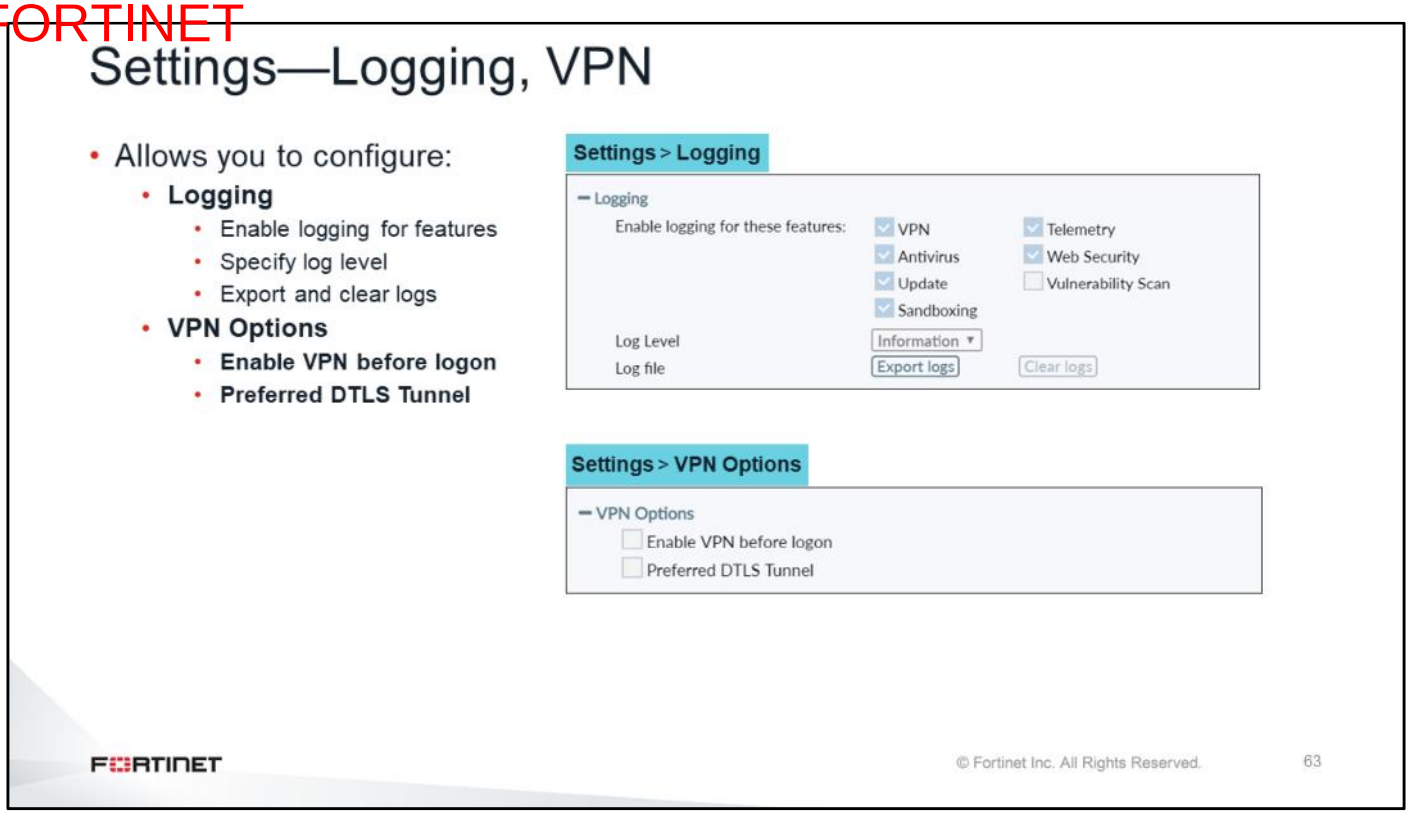
The additional settings tab on FortiClient allows you to configure system, logging, VPN options, and advanced settings.

You will explore these options in detail in this lesson.



There are additional settings available in the FortiClient system settings, which include:
Backup: You can back up the FortiClient configuration.
Restore: You can restore the FortiClient configuration.

Note that the FortiClient configuration file is an XML format configuration file. When performing a backup, you can select the file destination and save the file in an unencrypted (.conf) or encrypted format (.sconf). You can include or exclude comments in the XML configuration file.

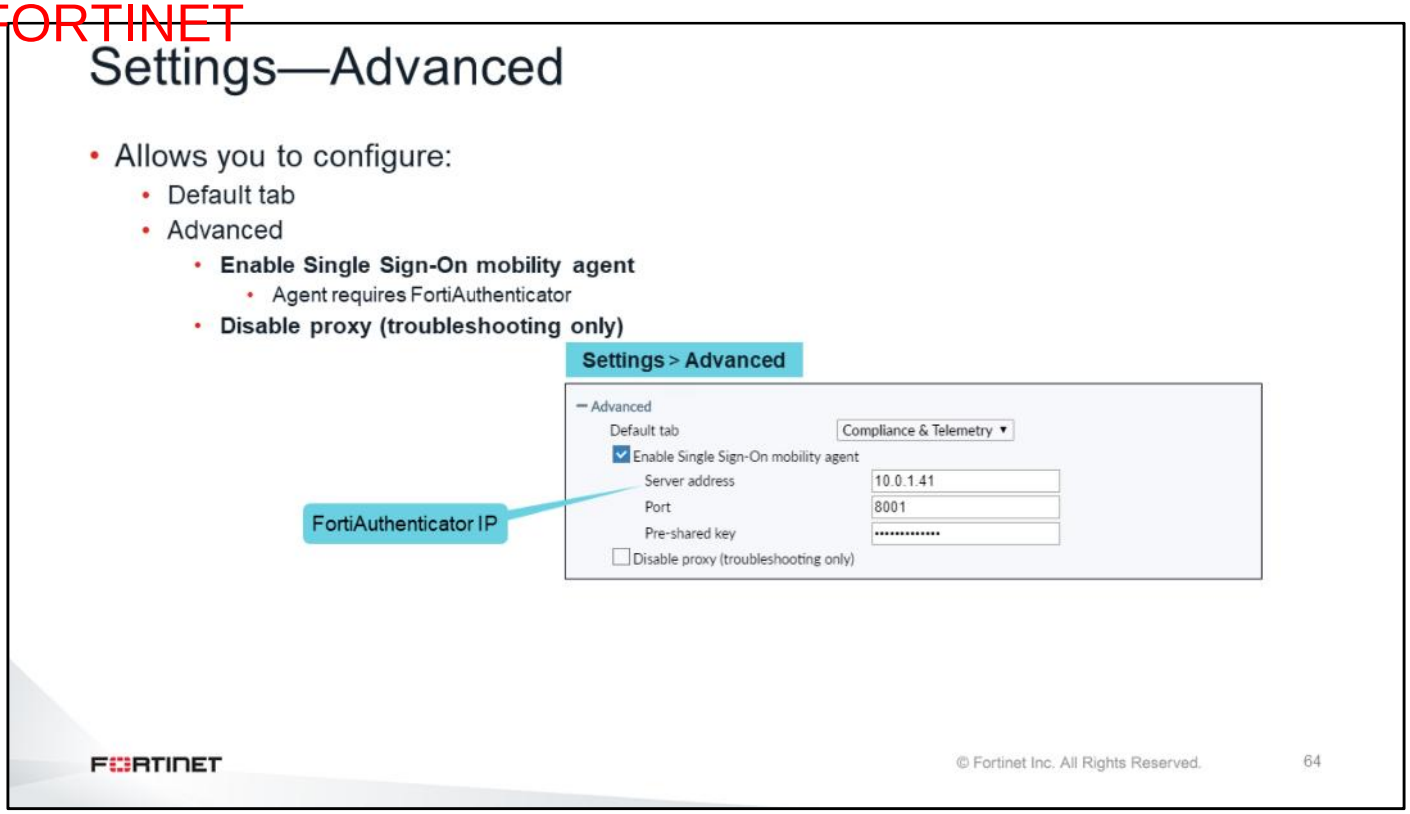


The **Logging** menu allows you to enable and disable logging for features (VPN, antivirus, web security, and update), specify log level, export logs, and clear logs. By default, logging for VPN, antivirus, web security, telemetry, vulnerability scan, sandboxing, and update are enabled. The default log level is **Information**.

The **VPN Options** drop-down list makes the **Enable VPN before logon** option available. On the Microsoft Windows side, in the User Accounts settings, the User must enter a user name and password to use this computer option.

You can also prefer DTLS over TLS by selecting **Preferred DTLS Tunnel**.

Note that the DTLS over TLS setting is only available for Windows endpoints.

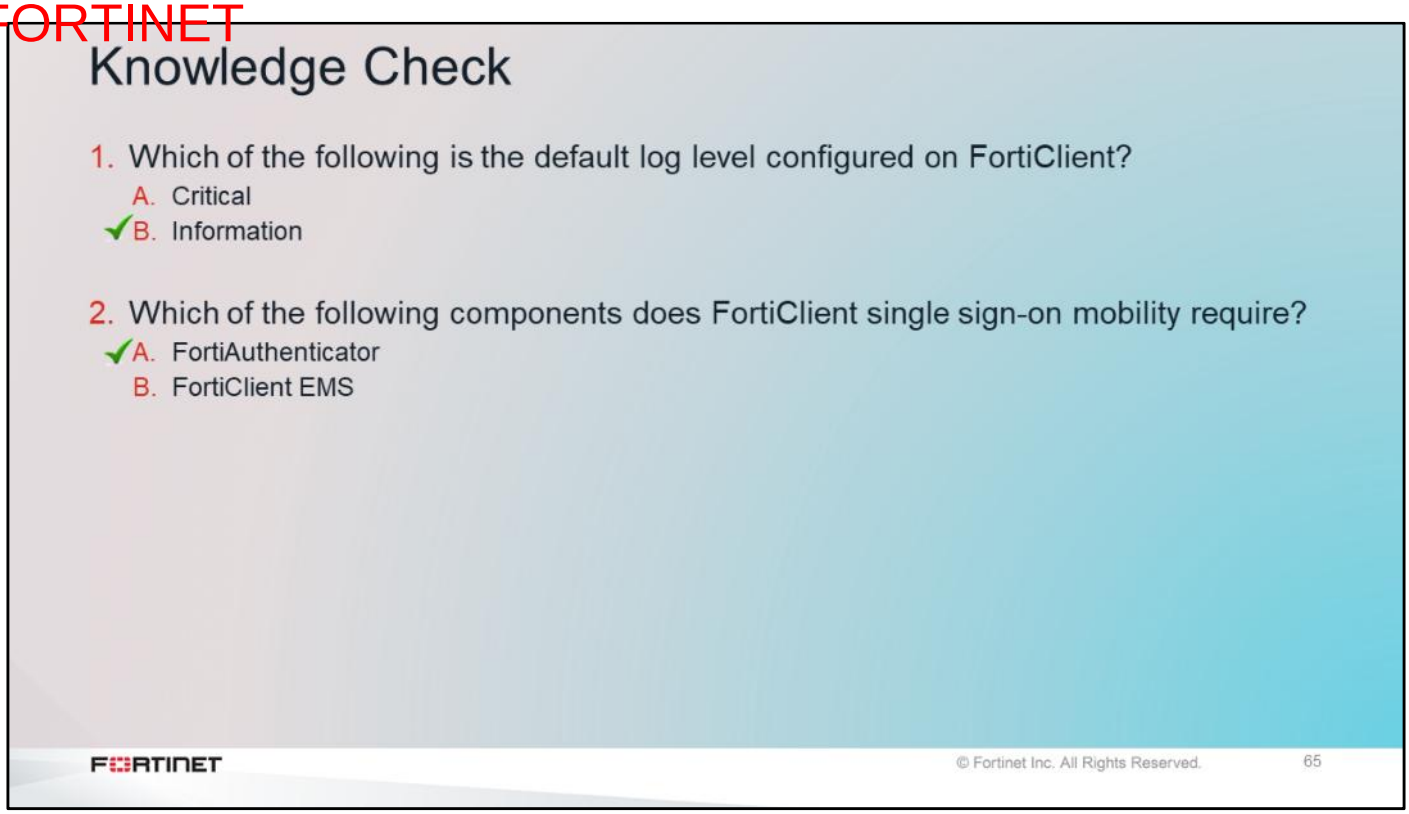


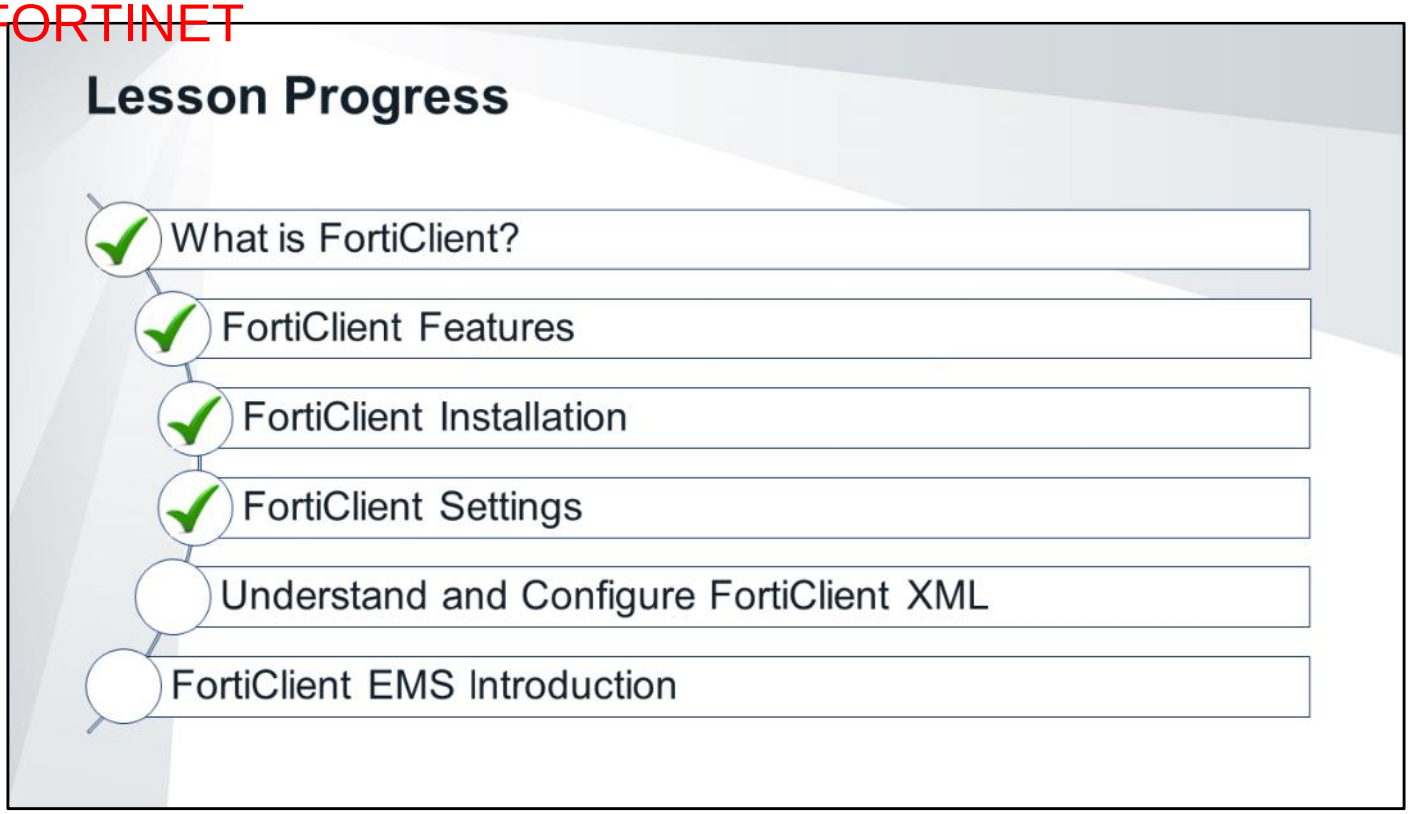
The **Advanced** menu allows you to enable:

- **Default tab**: You can select the default tab to display on FortiClient while on the launch console.
- **Enable Single Sign-On mobility agent**: Allows you to configure a single sign-on (SSO) mobility agent for FortiAuthenticator. You must apply a FortiClient SSO mobility agent license on your FortiAuthenticator device. The default port is set to 8001. The FortiAuthenticator listens on a configurable TCP port. FortiClient connects to FortiAuthenticator using TLS/SSL with two-way certificate authentication. The FortiClient sends a logon packet to FortiAuthenticator, which replies with an acknowledgement packet. FortiClient to FortiAuthenticator communication requires the following:

1. The IP address should be unique in the entire network.
2. FortiAuthenticator should be accessible from clients in all locations.
3. FortiAuthenticator should be accessible by all FortiGate devices.

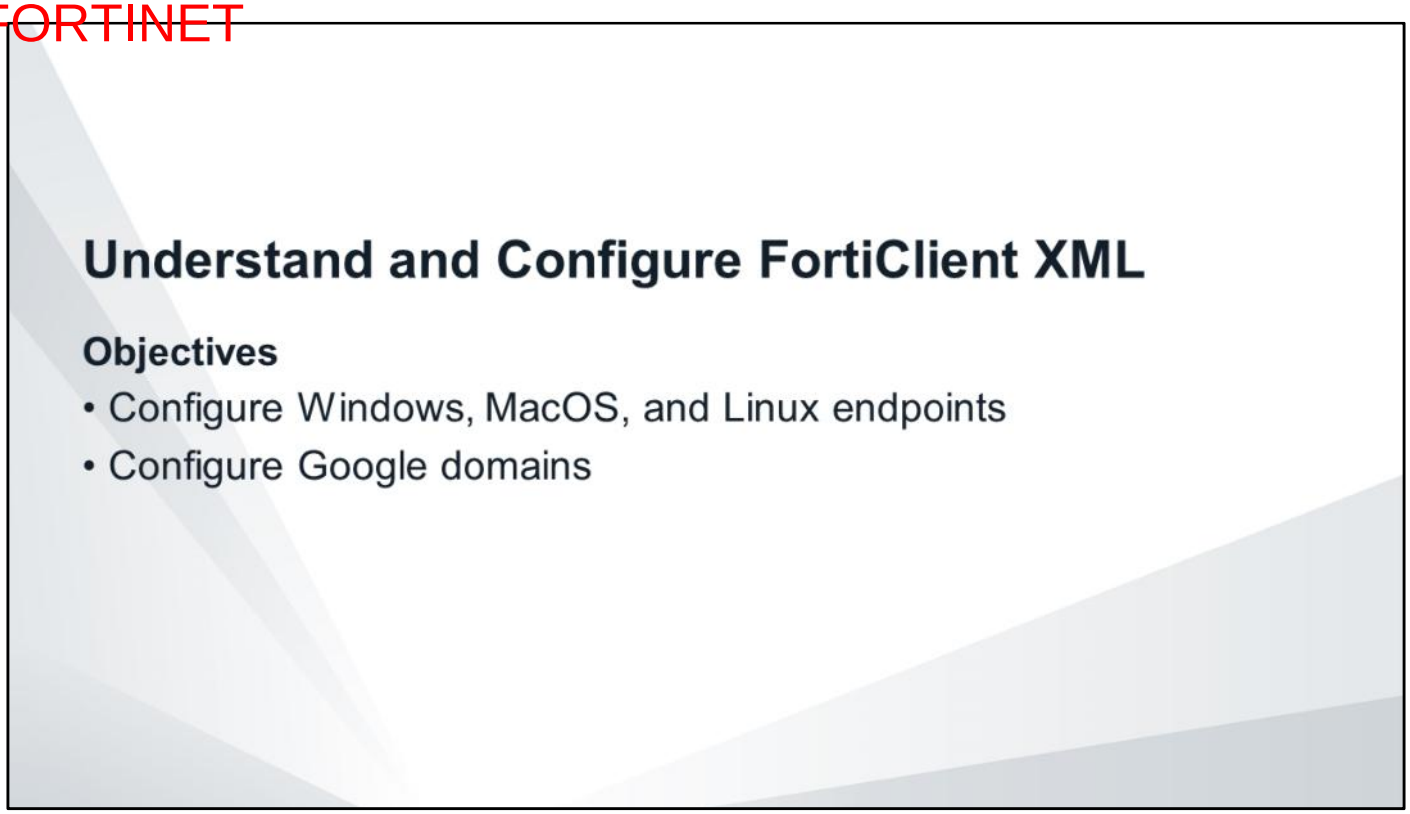
Note that the FortiClient SSO mobility agent requires a FortiAuthenticator running v2.0.0 or later, or v3.0.0 or later.





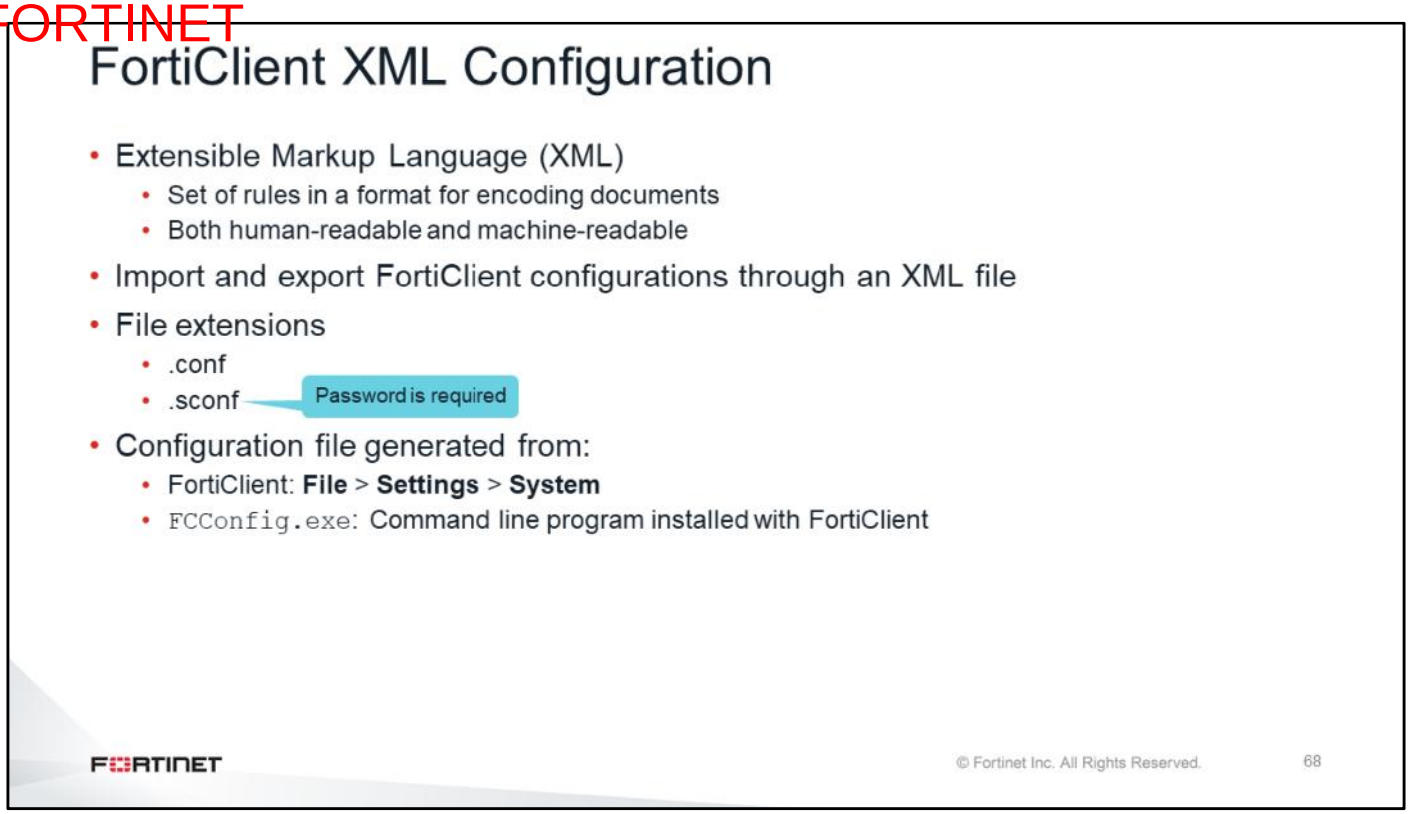
Good job! You now know FortiClient settings.

Now, you will learn how to configure FortiClient XML.



After completing this section, you should be able to achieve the objectives shown on this slide.

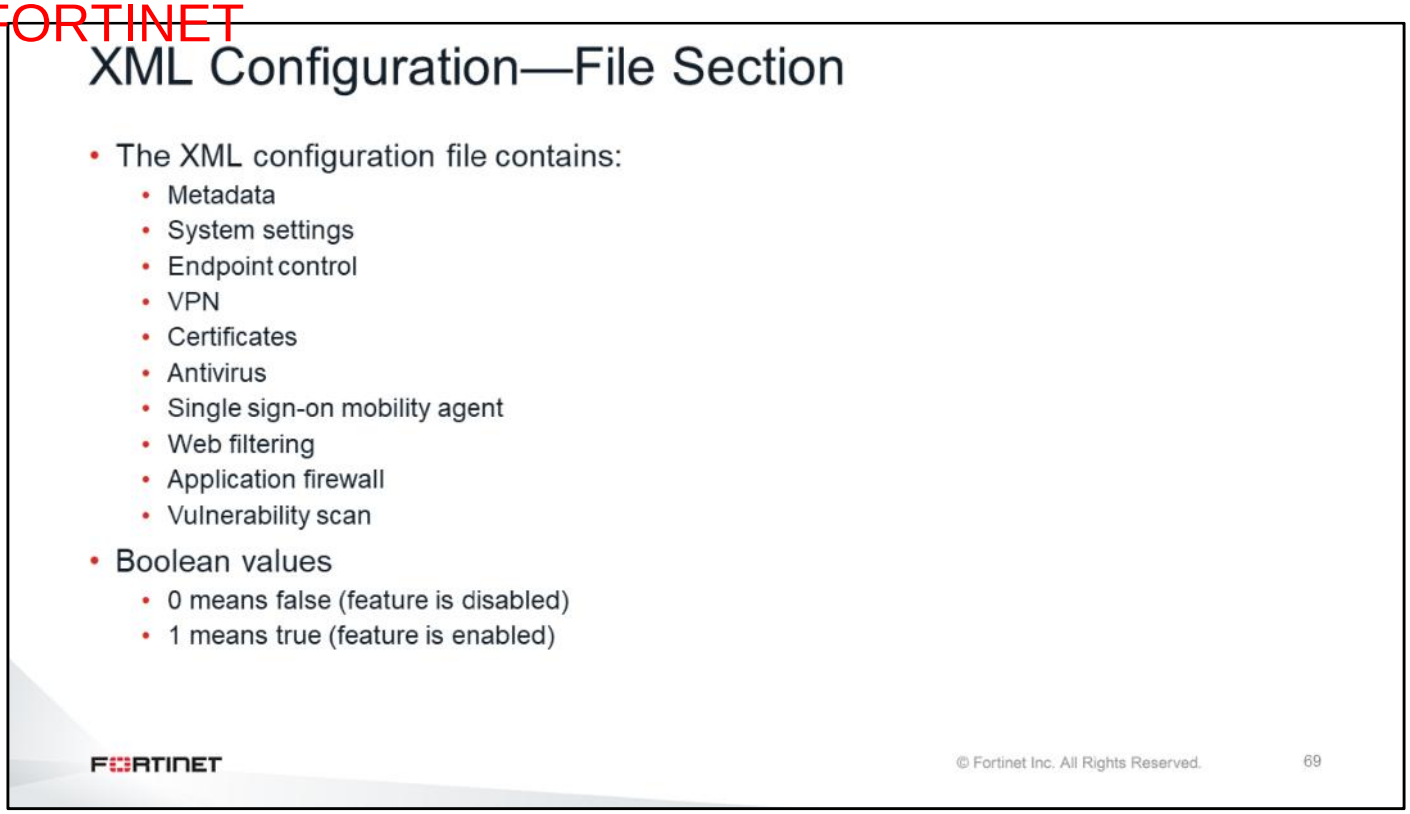
By demonstrating competence in configuring FortiClient XML, you will be able to configure FortiClient XML settings.



XML is a markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable.

FortiClient supports the importation and exportation of its configuration in an XML file, and supports two file types, which are:
- **.conf**: A plain-text configuration file.
- **.sconf**: A secure (encrypted) configuration file, which requires a password.

You can generate and back up a configuration file (which is an XML file) on the **Settings** page of the FortiClient dashboard, or by using the command-line program `FCConfig.exe`, which is installed with FortiClient.



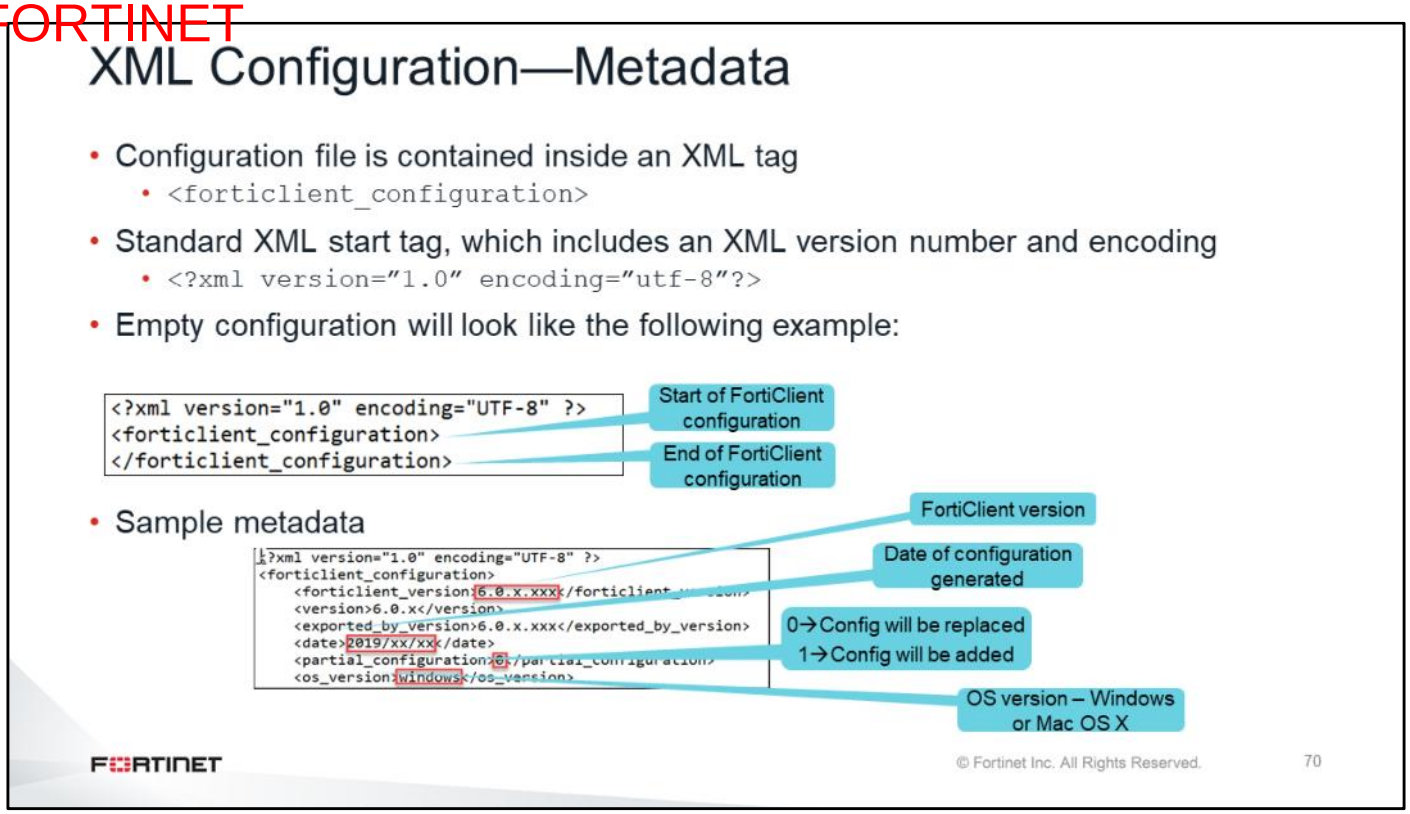
For the purpose of understanding the FortiClient XML configuration, the major section elements of the XML configuration are as follows:

- **Metadata**: Facilitates the discovery of relevant information and is the basic data controlling the entire configuration file.
- **System settings**: General settings that are not specific to any of the modules listed below (or affect more than one module)
- **Endpoint control**: Includes settings related to controlling endpoints, such as enable enforcement, off-net update, skip confirmation, disable unregister, silent registration, and so on.
- **VPN**: Includes settings related to global options that apply to both SSL VPN and IPsec VPN, and settings related to SSL VPN and IPsec VPN individually.

You can also configure XML for settings related to certificates, antivirus, single sign-on mobility agent, web filtering, application firewall, and vulnerability scan.

The XML configuration is controlled by two boolean values (usually denoted as true and false) that enable or disable a configuration setting—0 means false (feature is disabled), and 1 means true (feature is enabled).

Also in this lesson, you will learn how to enable and disable specific configuration settings.

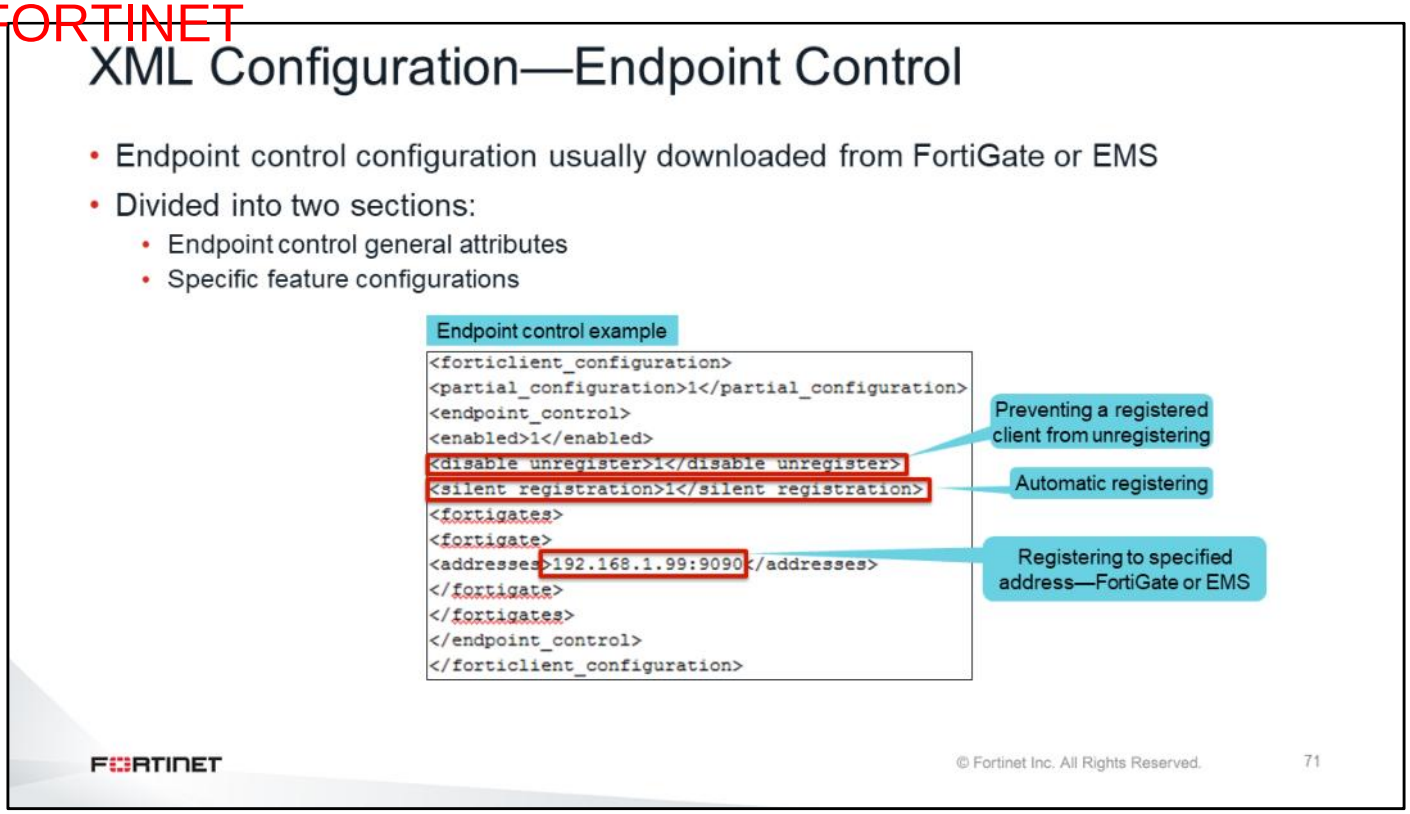


All of the XML tags and data in a configuration file are contained inside the XML tag `<forticlient_configuration>`. The first line of the configuration starts with a standard XML start tag `<?xml version="1.0" encoding="utf-8"?>`, which includes the XML version and encoding.

The XML configuration has elements (or nested child elements) that begin with a start tag and end with a matching end tag. An empty FortiClient configuration would look like what is shown on this slide.

If you export the configuration from FortiClient, it will include the FortiClient version, date of generation, and OS version (Windows or Mac OS X) from where the configuration was generated—either FortiGate or FortiClient EMS.

`<partial_configuration>` is a line of metadata that controls whether the configuration will be replaced or added in an import or restore. The value 0 will replace the configuration, and the value 1 will append the configuration to the existing configuration.



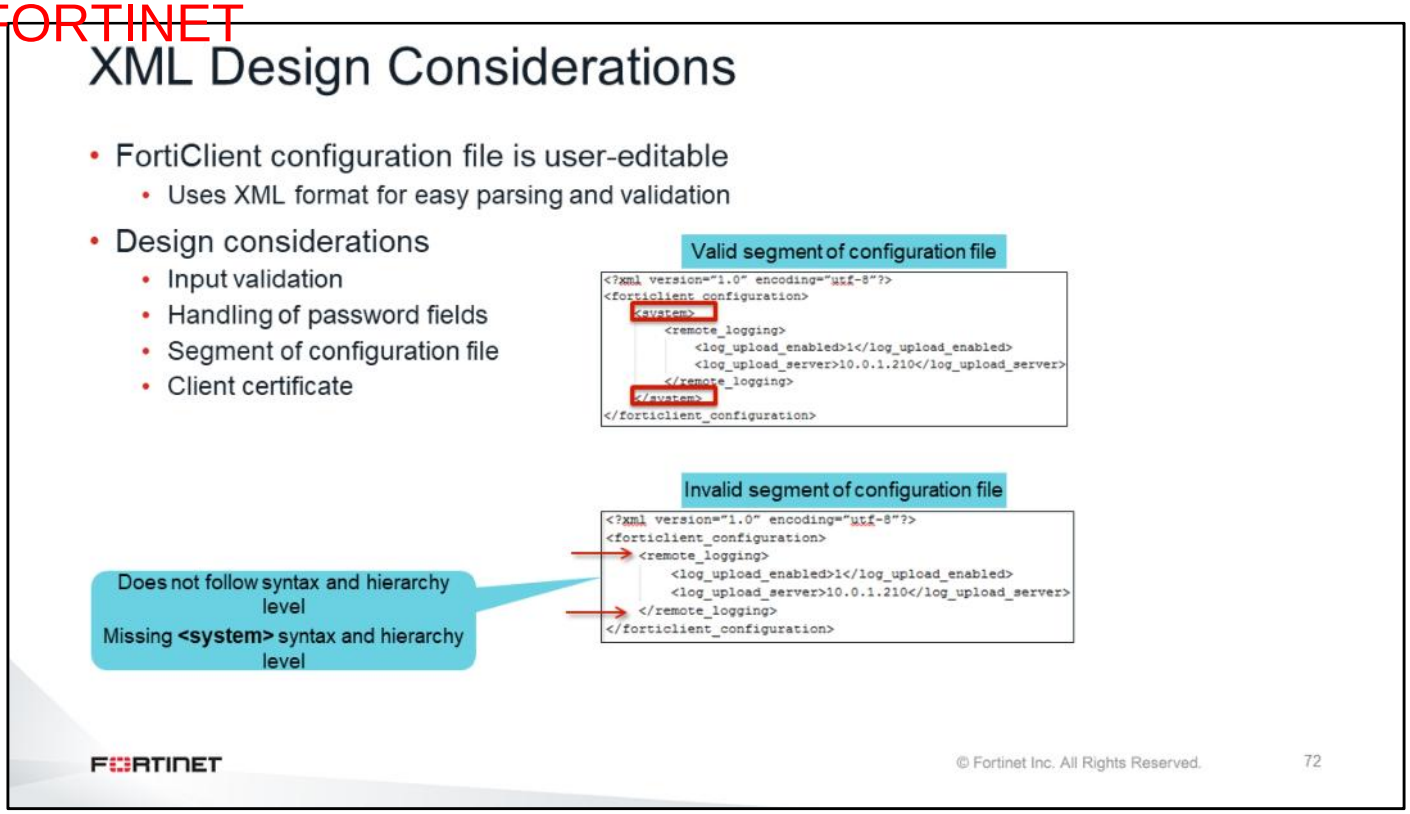
The endpoint control configuration element controls settings related to controlling endpoints, such as disable unregister, silent registration, enable enforcement, off-net update, skip confirmation, which features to display on the FortiClient console, and so on.

You usually download the endpoint control configurations from the FortiGate or EMS, or you can build it using the *XML Reference Guide* available at `http://docs.fortinet.com` in the FortiClient XML configuration section.
The endpoint control configurations are divided into two parts:

1. Endpoint control general attributes: These are contained in the <endpoint_control> XML tags.
2. Configuration details relating to specific FortiClient services, such as antivirus, web filtering, application firewall, vulnerability scanner, and so on. They are found in their respective configuration elements contained inside their XML tags. For example, the antivirus configuration is contained in the <antivirus> XML tags.

In the example shown on this slide, `silent_registration`, allows you to automatically register on FortiGate or FortiClient EMS without prompting the user to accept the registration. Silent registration is intended to be used with `disable_unregister`, which prevents a registered client from being able to unregister after successfully registering on a FortiGate or FortiClient EMS server.

The `addresses` XML setting defines that FortiClient will attempt to register on the first FortiGate or EMS listed here. You can add multiple IPs delimited with a semicolon.

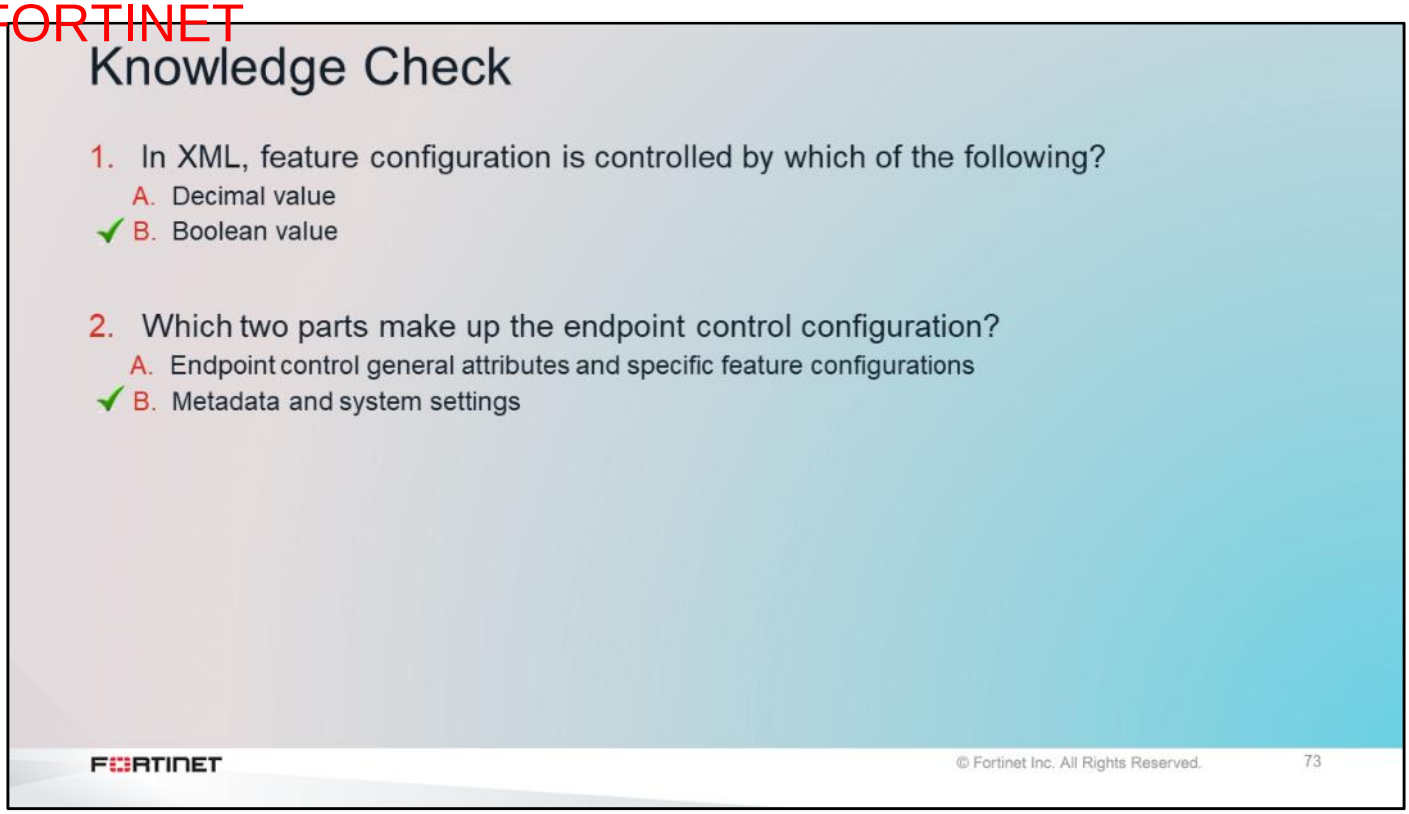


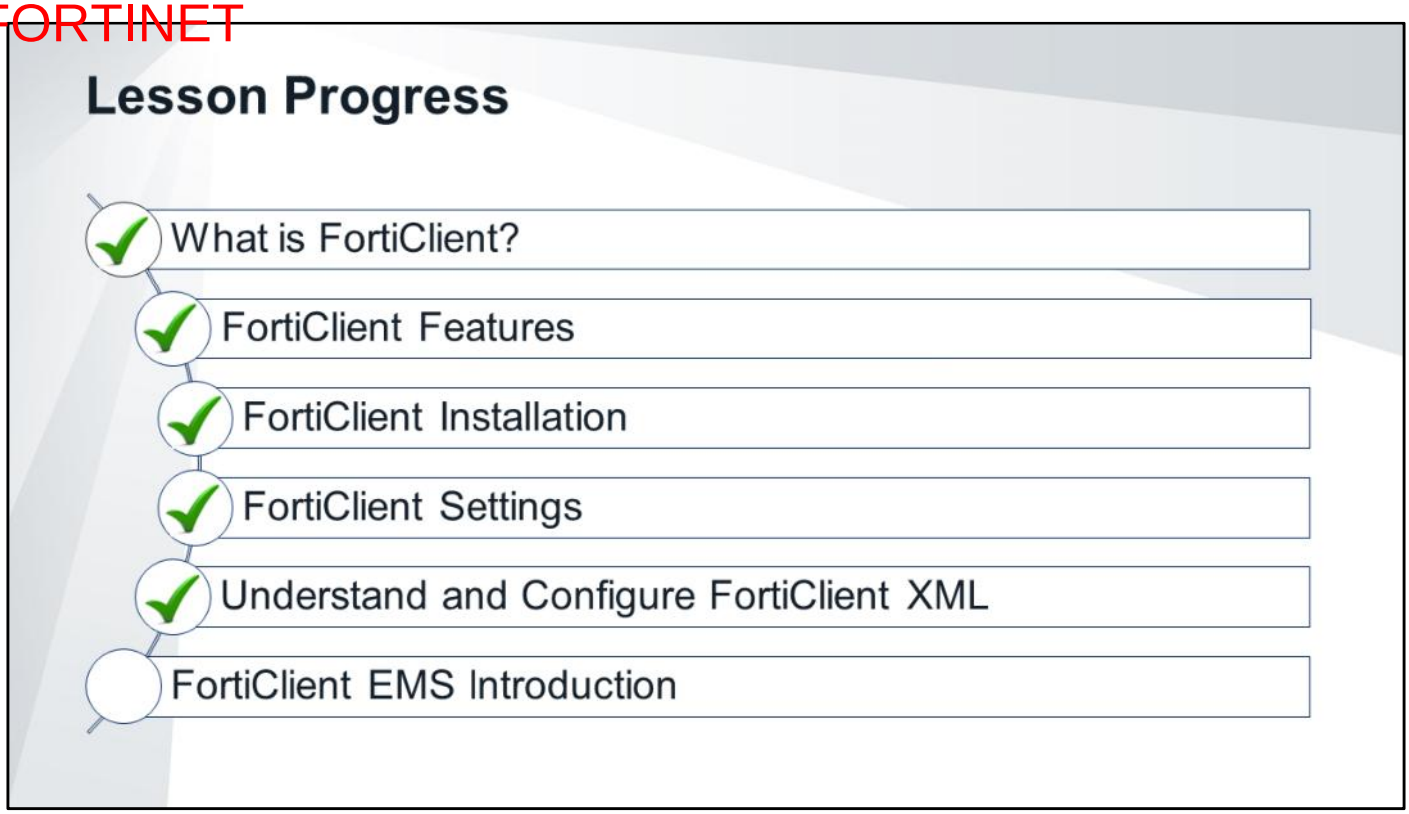
The FortiClient configuration file is user-editable and includes all client configurations. When building an XML configuration, you should adopt the following design considerations:

- **Input validation**: The import function performs basic validation, and writes to a log when errors or warnings are found. The default values for omitted configurations are ignored, but for VPN they are defined in the configuration.
- **Handling of password fields**: The password and username fields will be encrypted (prefixed with “Enc”) when a configuration is exported. However, the import function is able to take either the clear text or encrypted format.
- **Segment of configuration file**: The XML configuration allows you to import the segment (partial configuration) of a configuration file. However, the segment should follow the syntax and hierarchy defined in the *XML Reference Guide* available at `http://docs.fortinet.com`.

In the example, the `invalid segment configuration` file is missing the hierarchy and syntax for `<system>` level commands and is considered to be an invalid segment.

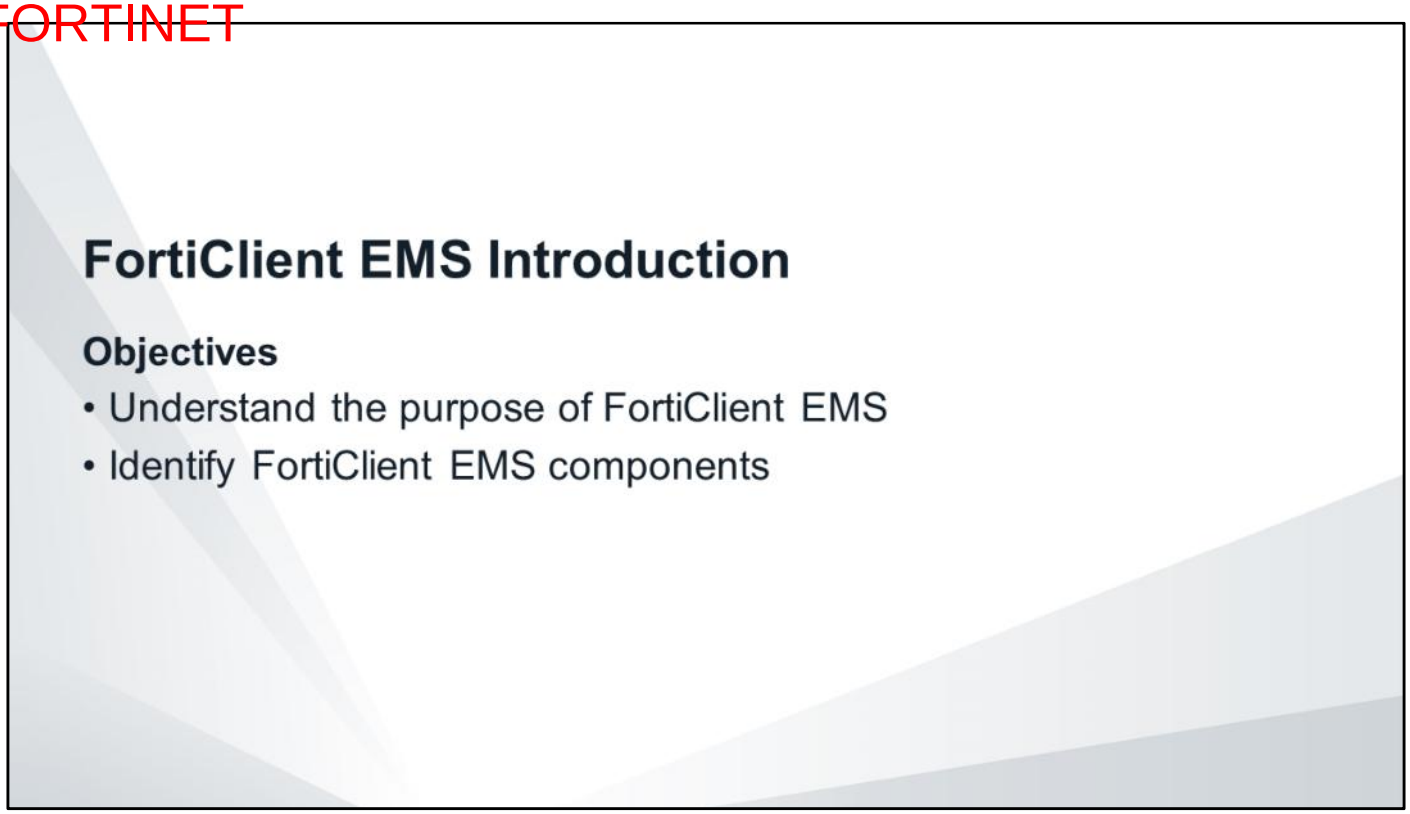
Client certificate: Client certificates are exported in an encrypted format in the configuration file.





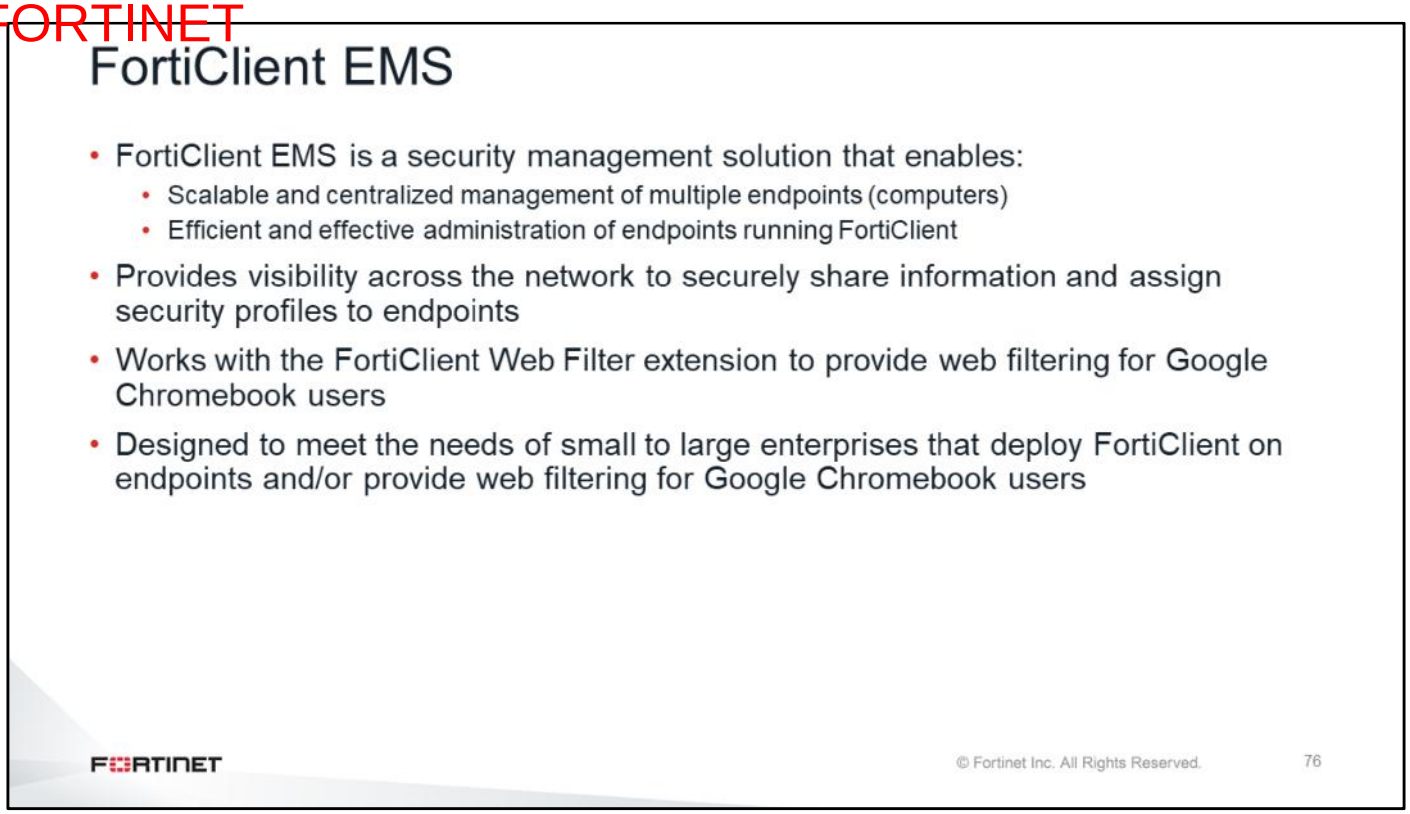
Good job! You now know how to configure FortiClient XML.

Now, you will learn about FortiClient EMS.



After completing this section, you should be able to achieve the objectives shown on this slide.

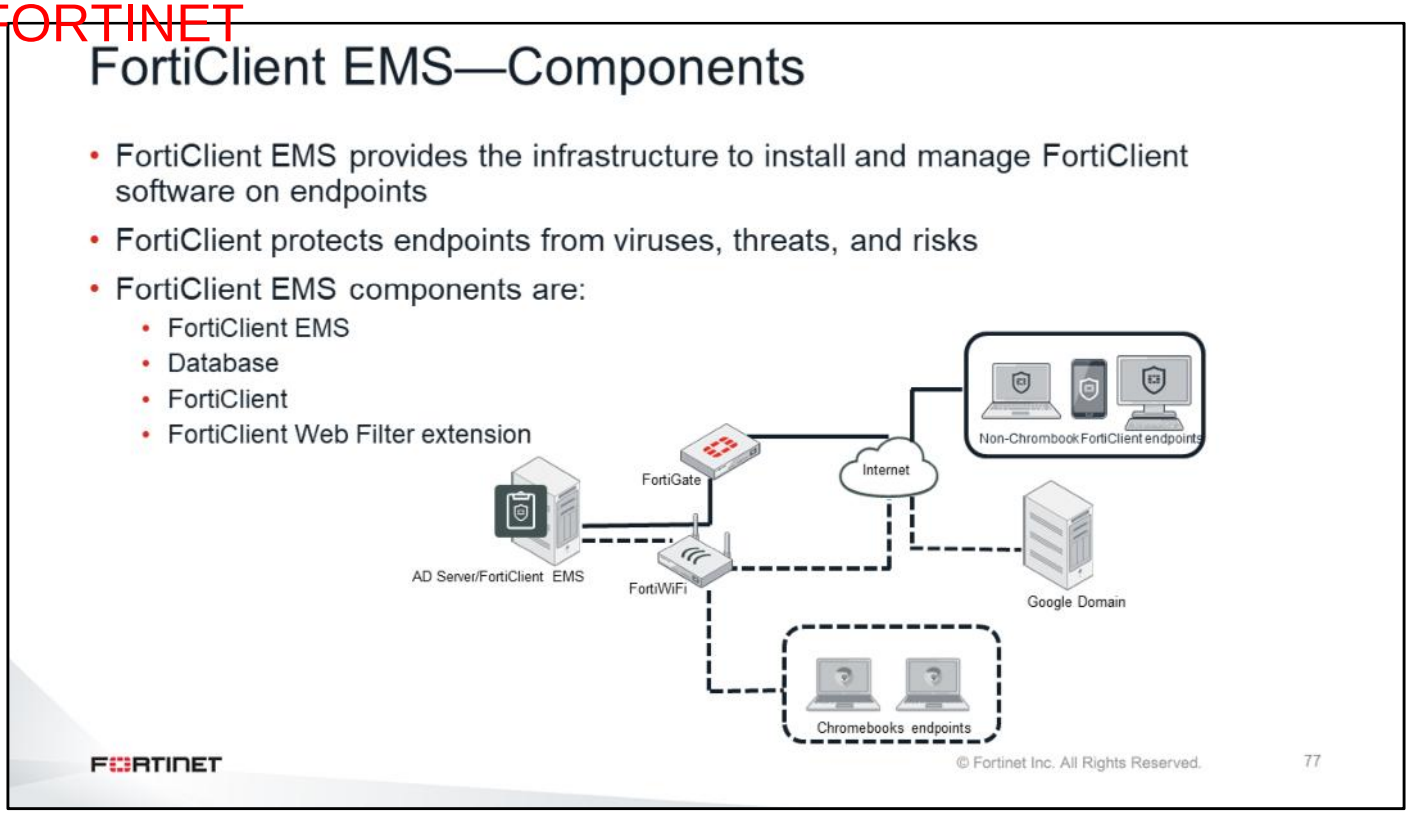
By demonstrating competence in understanding the components and management functions of FortiClient EMS, you will be able to understand the purpose of FortiClient EMS.



FortiClient EMS is a security management solution that enables scalable and centralized management of multiple endpoints (computers). It also provides efficient and effective administration of endpoints running FortiClient, and visibility across the network to securely share information and assign security profiles to endpoints. It is designed to maximize operational efficiency and includes automated capabilities for device management and troubleshooting.
FortiClient EMS also works with the FortiClient Web Filter extension to provide web filtering for Google Chromebook users.

The benefits of deploying FortiClient EMS include:
- Remotely deploying FortiClient software to Windows computers
- Updating profiles for endpoint users regardless of access location
- Administering FortiClient endpoint connections, such as accepting, disconnecting, and blocking connections
- Managing and monitoring endpoints, such as status, system, and signature information
- Identifying outdated versions of FortiClient software
- Defining web filtering rules in a profile and remotely deploying the profile to the FortiClient Web Filter extension on Google Chromebook endpoints

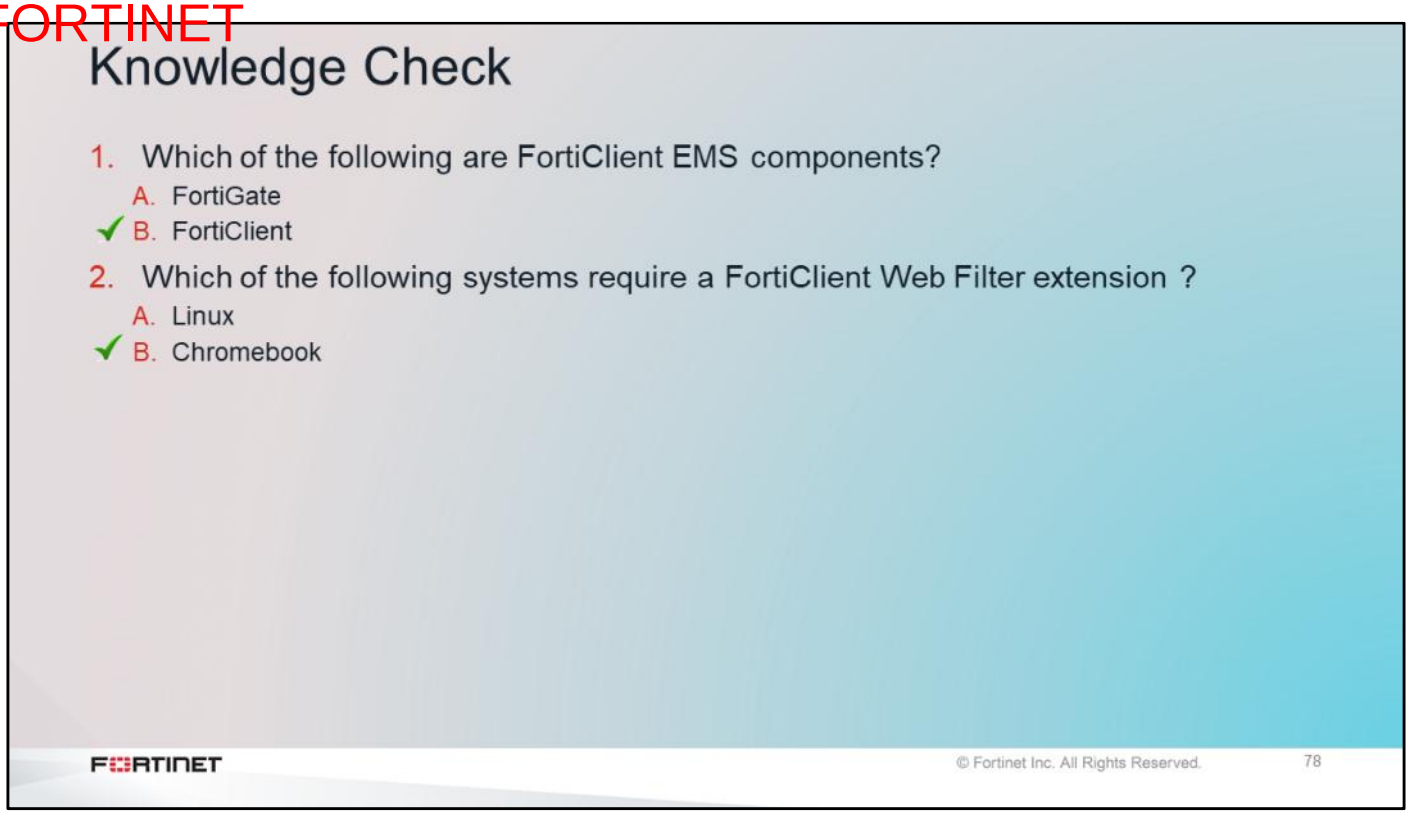
You can manage endpoint security for Windows and macOS platforms using a unified organizational security policy. An organizational security policy provides a full, understandable view of the security policies defined in the organization. You can see all policy rules, assignments, and exceptions in a single unified view. FortiClient EMS is part of the Fortinet Endpoint Security Management suite, which ensures comprehensive policy administration and enforcement for an enterprise network.

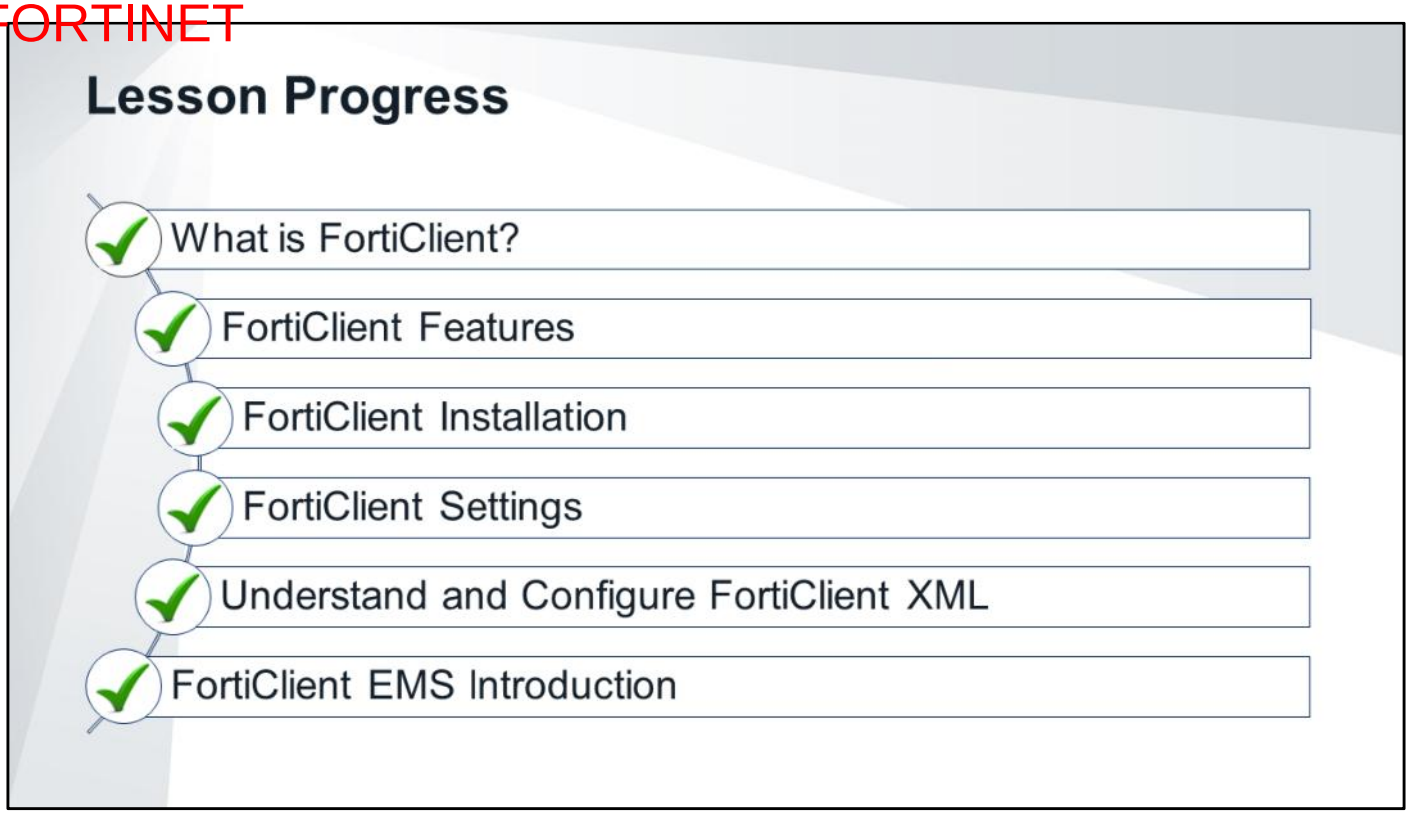


The following components make up FortiClient EMS:

- **FortiClient EMS**: Manages FortiClient on endpoints that connect to your network. It also manages the FortiClient Web Filter extension installed on Google Chromebook endpoints, which are connected to your Google domain. It includes two types of software:
- Console software that manages security profiles, FortiClient on endpoints, and Chromebook endpoints
- Server software that provides secure communication between endpoints and the console and between Chromebook endpoints and the Google Admin console
- **Database**: Stores security profiles and events. Also stores user information retrieved from the Google Admin console for Chromebooks. The SQL database is installed as part of the FortiClient EMS installation
- **FortiClient**: Helps enforce security and protection on endpoints. It runs on servers, desktops, and portable computers you want to secure
- **FortiClient Web Filter extension**: Communicates with FortiClient EMS and enforces web filtering on Google Chromebook endpoints

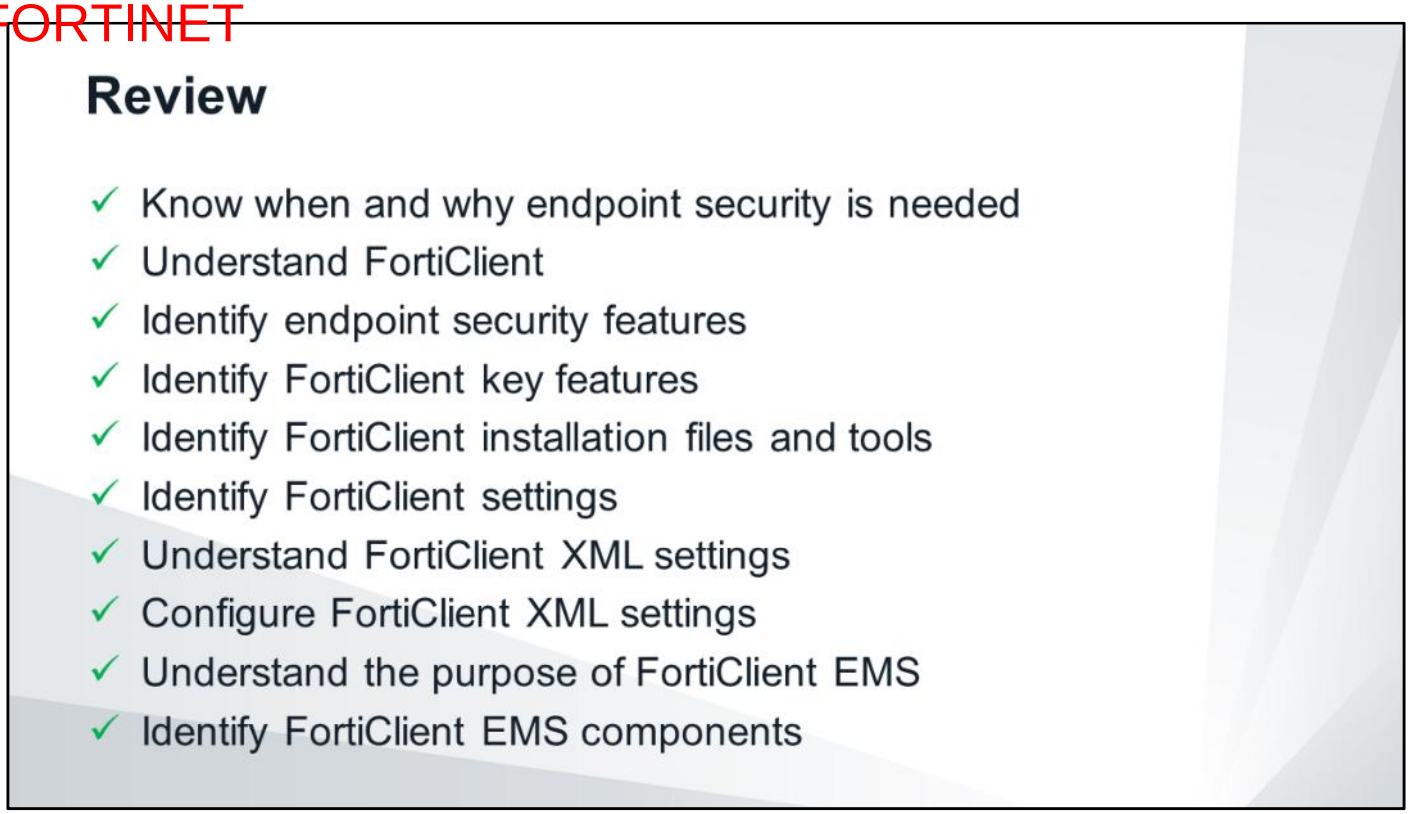
In the next lesson, we will discuss the FortiClient EMS in more detail, and explore all the features and options.





Congratulations! You have completed this lesson.

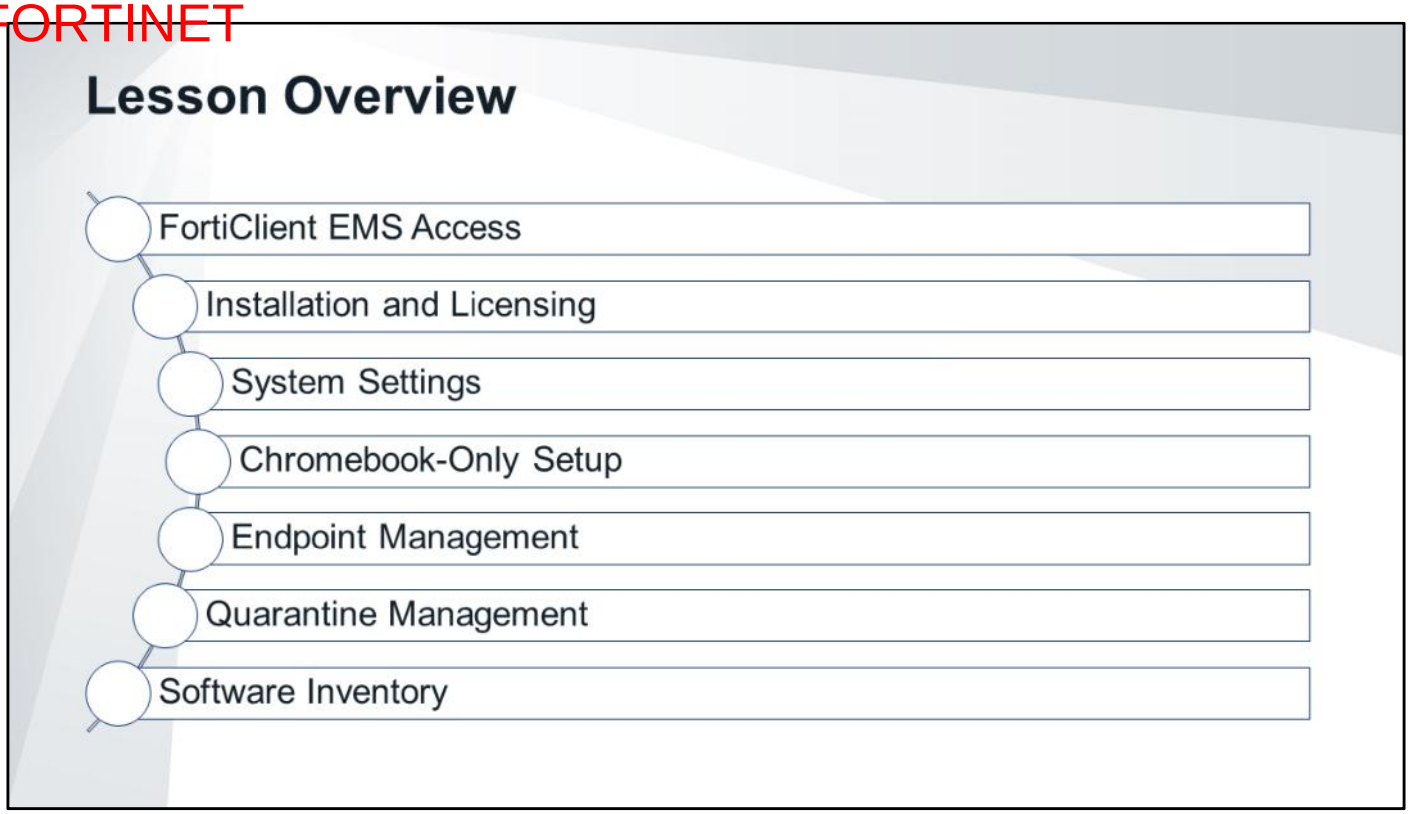
Now, you will review the objectives that you covered in this lesson.



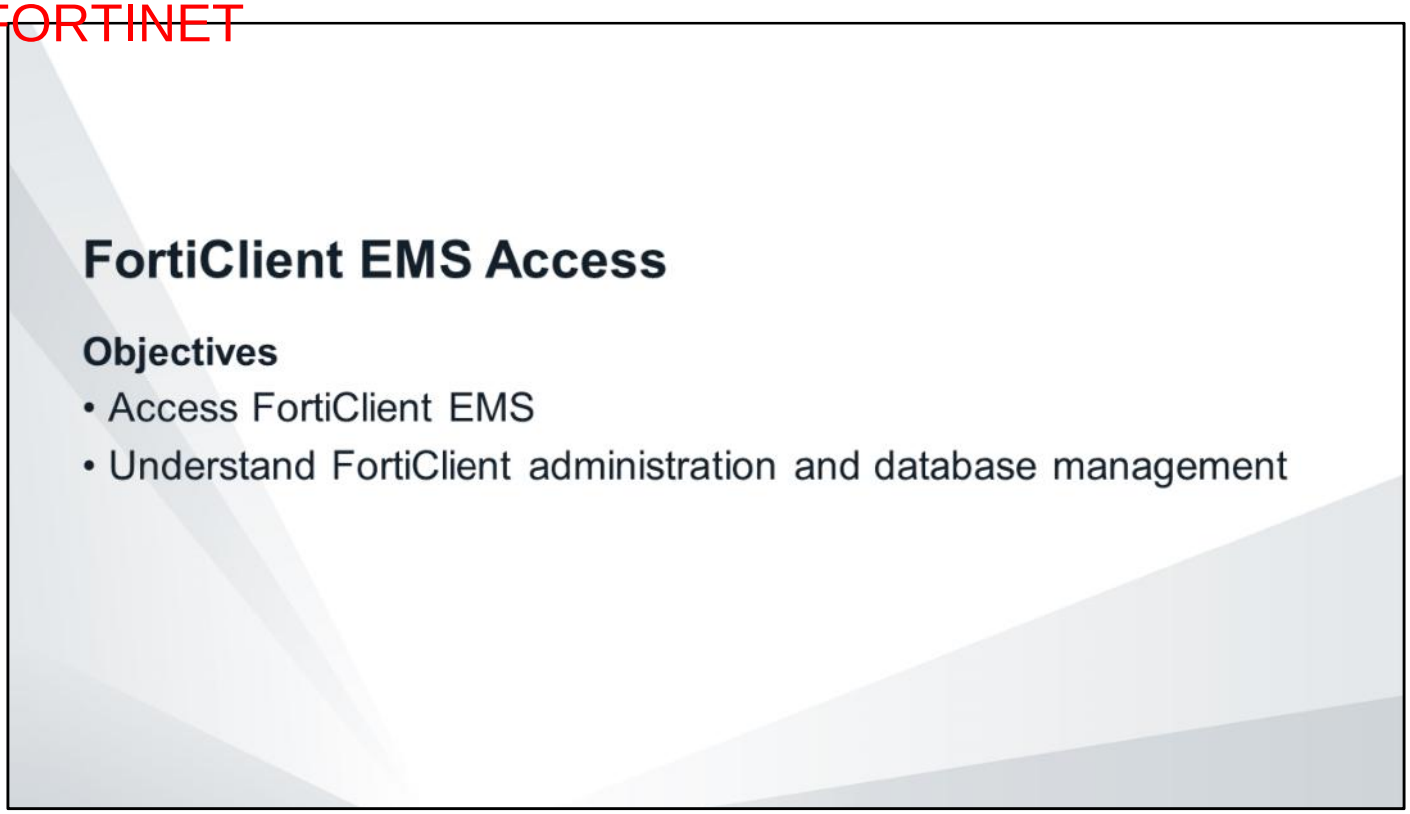
This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to use FortiClient features and options to install and use FortiClient to secure endpoints in your network.

In this lesson, you will learn how to install, configure, and administer FortiClient EMS. You will also learn how to manage a large number of endpoints.

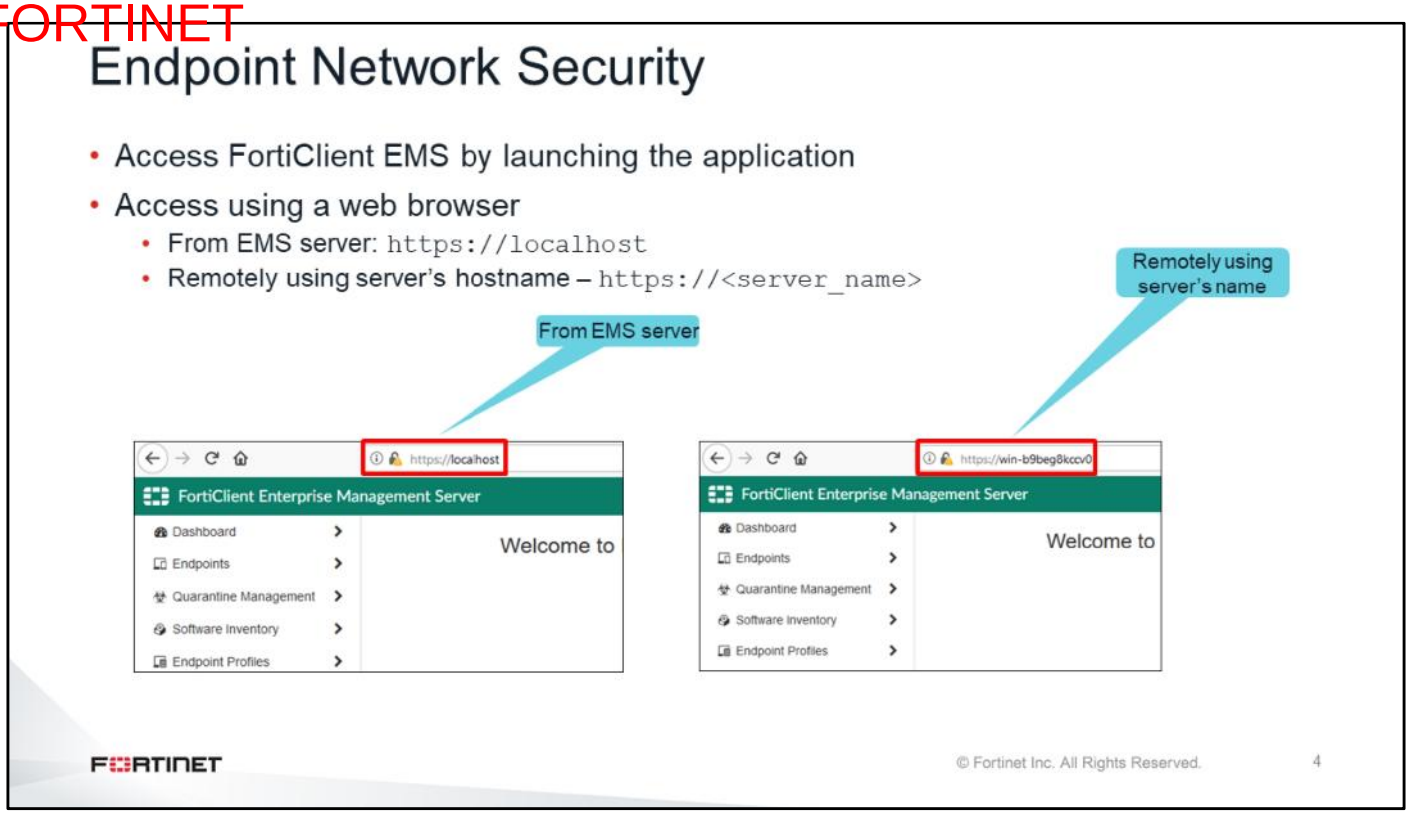


In this lesson, you will learn about the topics shown on this slide.



After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in understanding the management functions of FortiClient EMS, you will be able to understand the FortiClient EMS administration and database management, and identify its components.



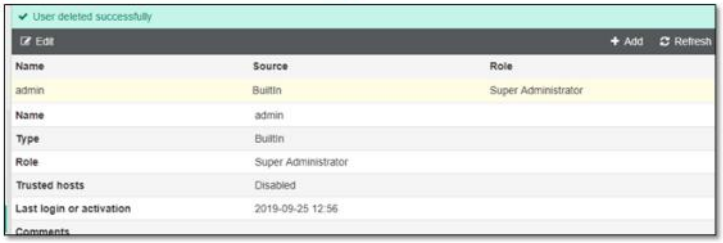
There are multiple ways to access FortiClient EMS. You can access FortiClientEMS by launching the FortiClient EMS application or by using a supported web browser. On the EMS server, type `access localhost via https` in the web browser, and, if accessing remotely, use the server's hostname or FQDN to access the page over the web.

Tip: You can get the server name by running the command `ipconfig /all` on the server. The host name will appear in the Windows IP configuration. If you are unable to access the server remotely, make sure you are able to ping `servername`, which you can do by adding it to the DNS entry or Windows host file. You may have to modify the firewall rules to allow the connection.

FortiClient EMS—Administration

- Default user account is admin
  - It has complete access to all FortiClient EMS permissions, including modification, user permissions, approval, discovery, and deployment
  - The admin user has access to all configured Windows and LDAP servers and users, and has the authority to configure user privileges and permissions
  - By default, the admin user account has no password; you should add a password to increase security
- You can view the default admin account and all users added to FortiClient EMS on

Administration > Administrators

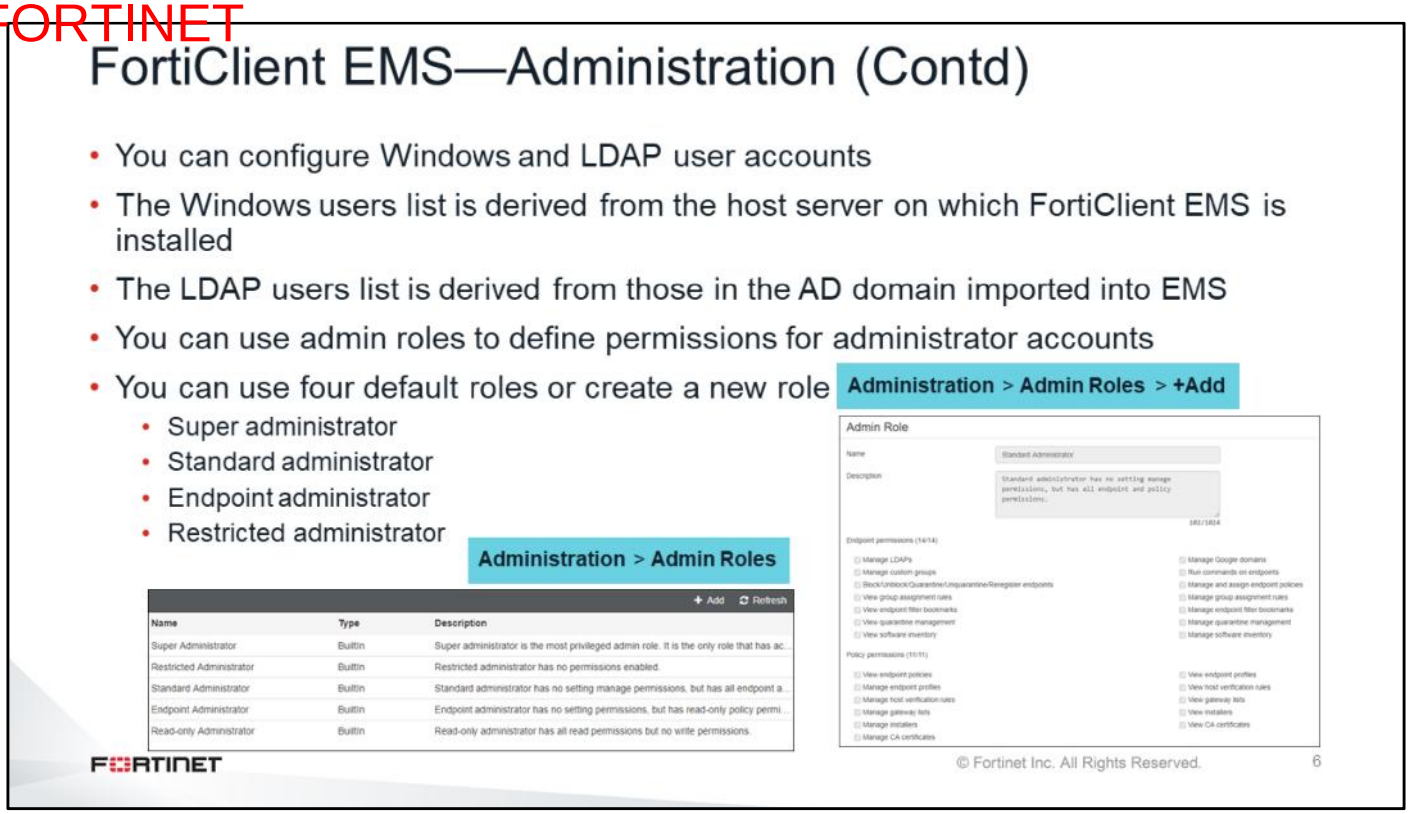


FORTINET

5

The default user named *admin* has complete access to all FortiClient EMS permissions, including modification, user permissions, approval, discovery, and deployment. The admin user has access to all configured Windows and LDAP servers and users, and has the authority to configure user privileges and permissions. If you are not authorized for certain tasks or devices, the related menu items, items in content pages, and buttons are hidden or disabled. In addition, a message informs you that you do not have permission to view the selected information or perform the selected operation.

By default, the admin user account has no password; you should add a password to increase security.

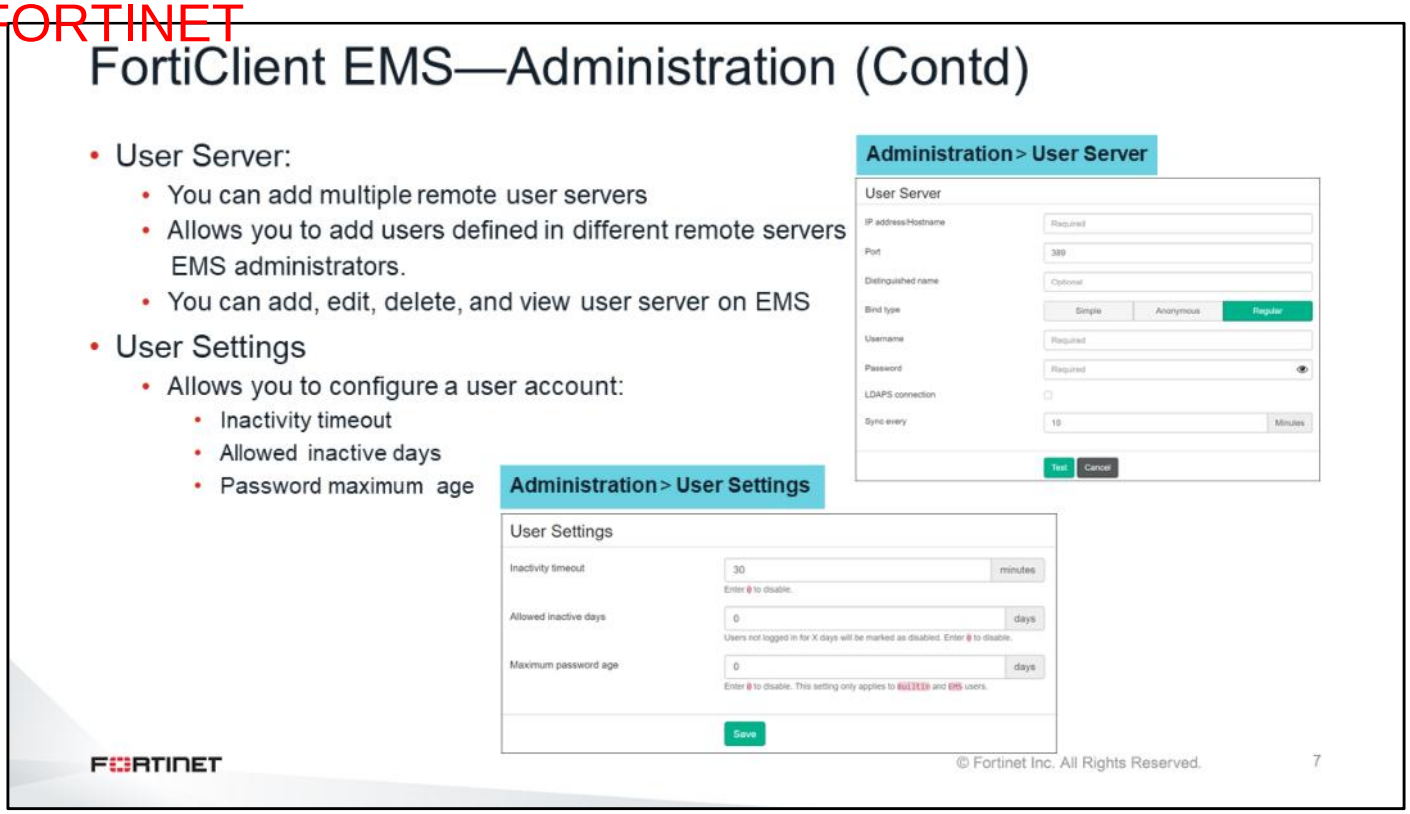


You can configure Windows and LDAP admin user accounts. The Windows users list is derived from the host server on which FortiClient EMS is installed. The LDAP users list is derived from those in the AD domain imported into EMS.

You can use admin roles to define the permissions each administrator account has in FortiClient EMS. You can use one of the four default admin roles in FortiClient EMS (super administrator, standard administrator, endpoint administrator, restricted administrator) or create a new admin role to assign to an administrator account.

Super administrator: This role is the most privileged admin role. This role has complete access to all FortiClient EMS permissions, including modification, user permissions, approval, discovery, and deployment. This is the only built-in role that has access to the Administration section of the GUI. This role has access to all configured Windows and LDAP servers and users, and has the authority to configure user privileges and permissions. The default admin account is configured as a super administrator and cannot be changed to another admin role.
Standard administrator: This role includes all endpoint and policy permissions, and read-only permissions to settings permissions.
Endpoint administrator: This role includes all endpoint permissions and read-only permissions to policy and settings permissions.
Restricted administrator: This role has no permissions enabled.

Each admin role can include permissions from three categories: endpoint permissions, policy permissions, and settings permissions. For admin roles that are not authorized for certain tasks or devices, EMS hides or disables the related menu items, items in content pages, and buttons.

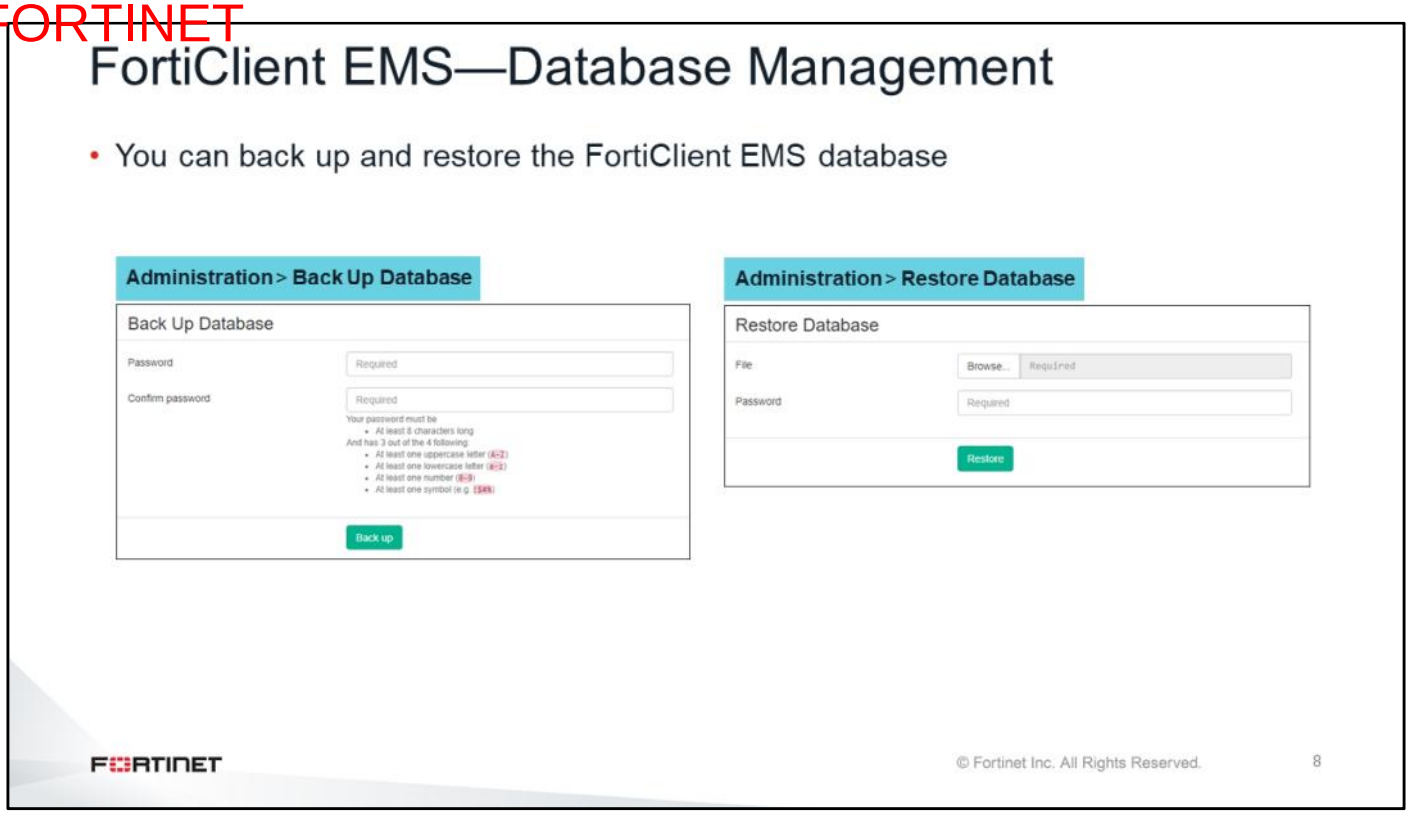


You can add multiple remote user servers to EMS. This allows you to add users defined in different remote servers as EMS administrators. To add a user server, configure the options that are shown in this slide. After you have added the user server, you can edit, delete and view server details. When you click **Administration** > **User Server**, **User Server** window, displays a list of configured servers, and its domain name, NetBIOS name, user count, last sync, sync every, address, distinguished name, and username.

You can also configure user settings on EMS. The Inactivity timeout setting specifies how long to keep inactive users logged into FortiClient EMS. When the time expires, EMS automatically logs the user out. To keep inactive users logged into FortiClient EMS indefinitely, type a value of 0.

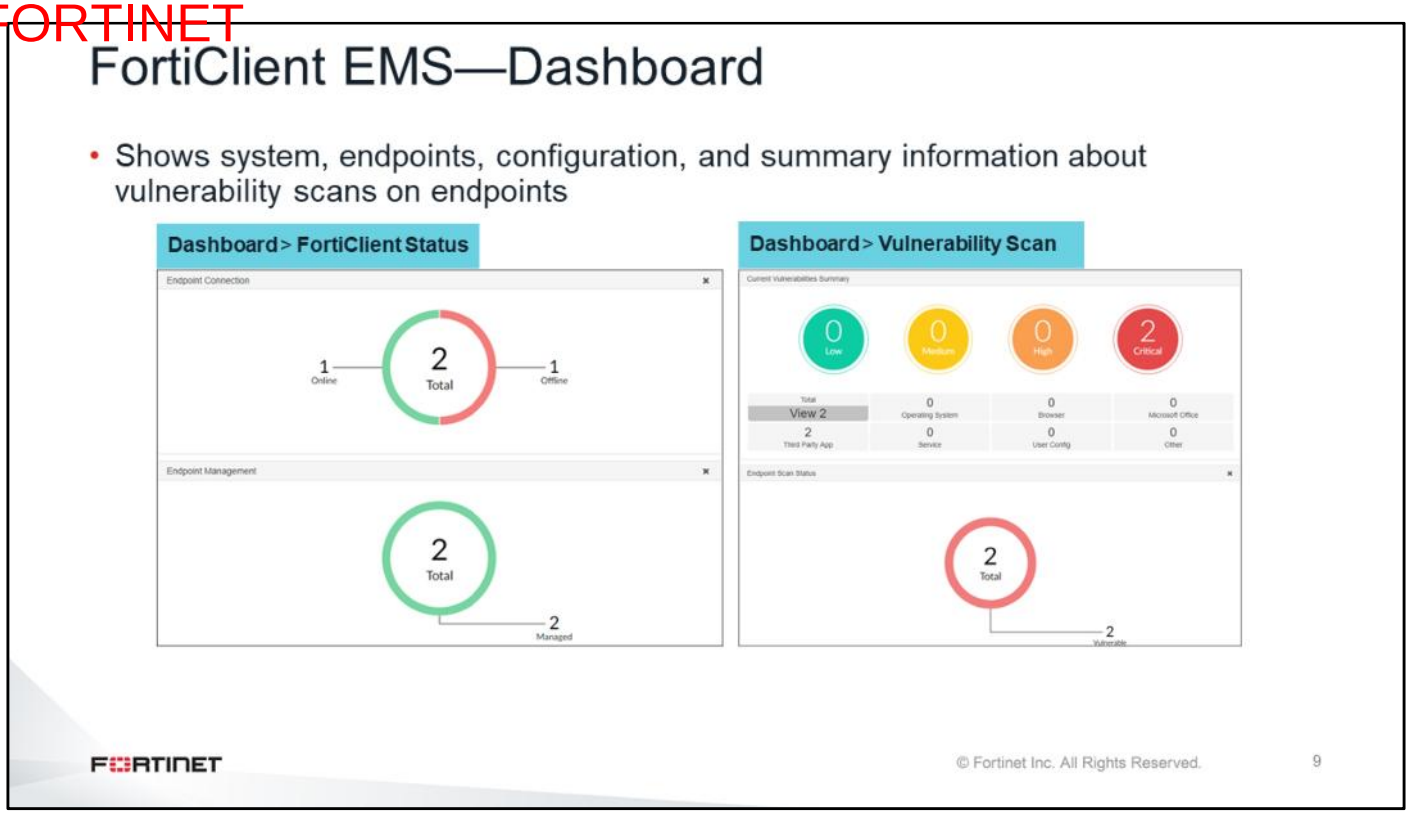
The Allowed inactive days setting specifies the number of days of inactivity after which to disable a user account. For example, if this field is set to `10` and a user does not log into FortiClient EMS for ten days, EMS disables their account so that they cannot log into FortiClient EMS. A user with super administrator permissions can reactivate their account.

Maximum password age setting specifies the number of days after which the user is forced to change their password. To disable this setting, type in a value of 0.. This setting only applies to built-in users such as the admin user and EMS users.



FortiClient database management allows you to back up and restore the database, as shown in this slide. The options are available in FortiClient EMS **Administration** window. A password is required to take a backup, same password will be used to restore database using the same backup. When the database is restored, a message appears. The message instructs you to wait for the restored database to reload. You must wait until it is completely restored.

Note that restore will work only if the database was backed up using the same version number.

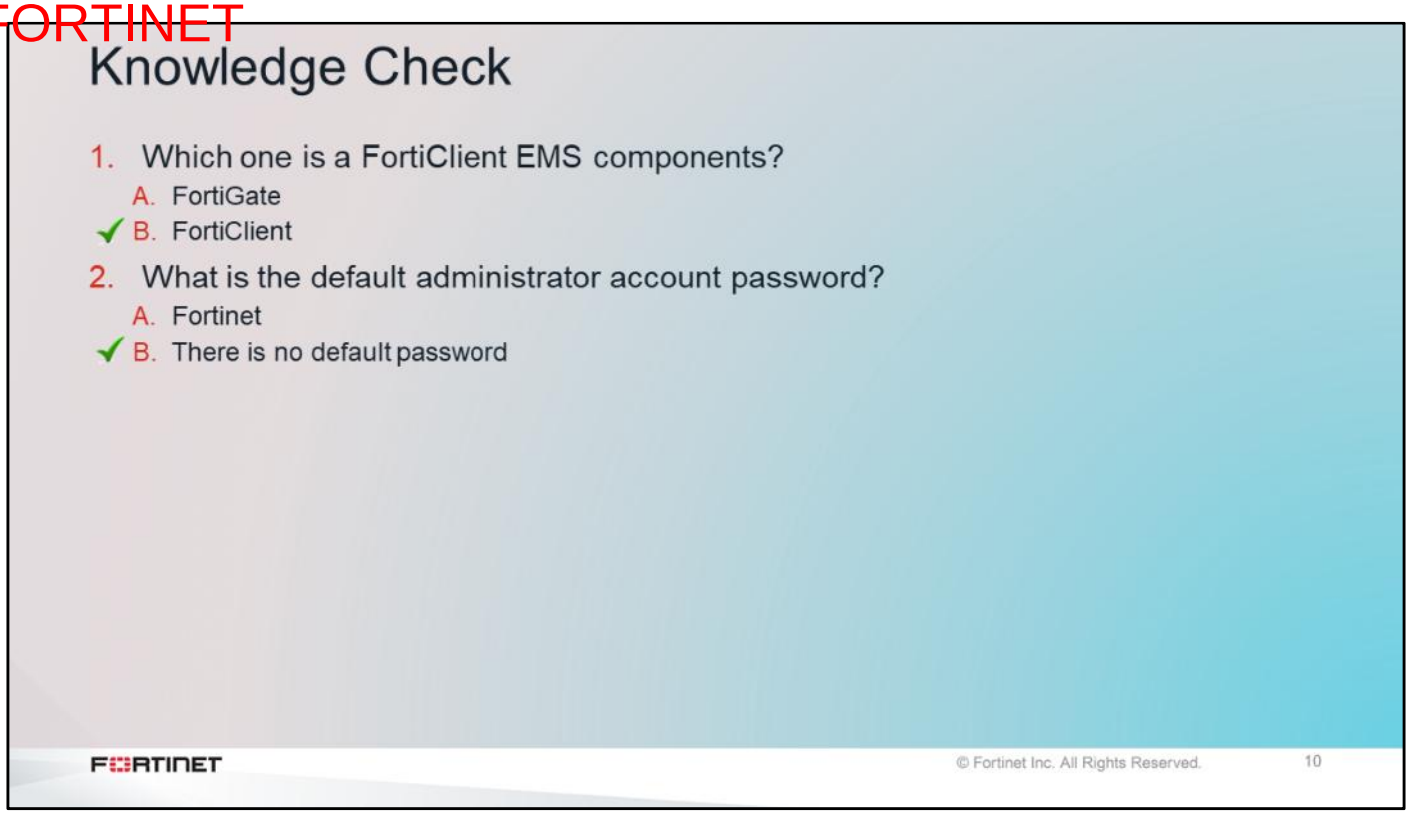


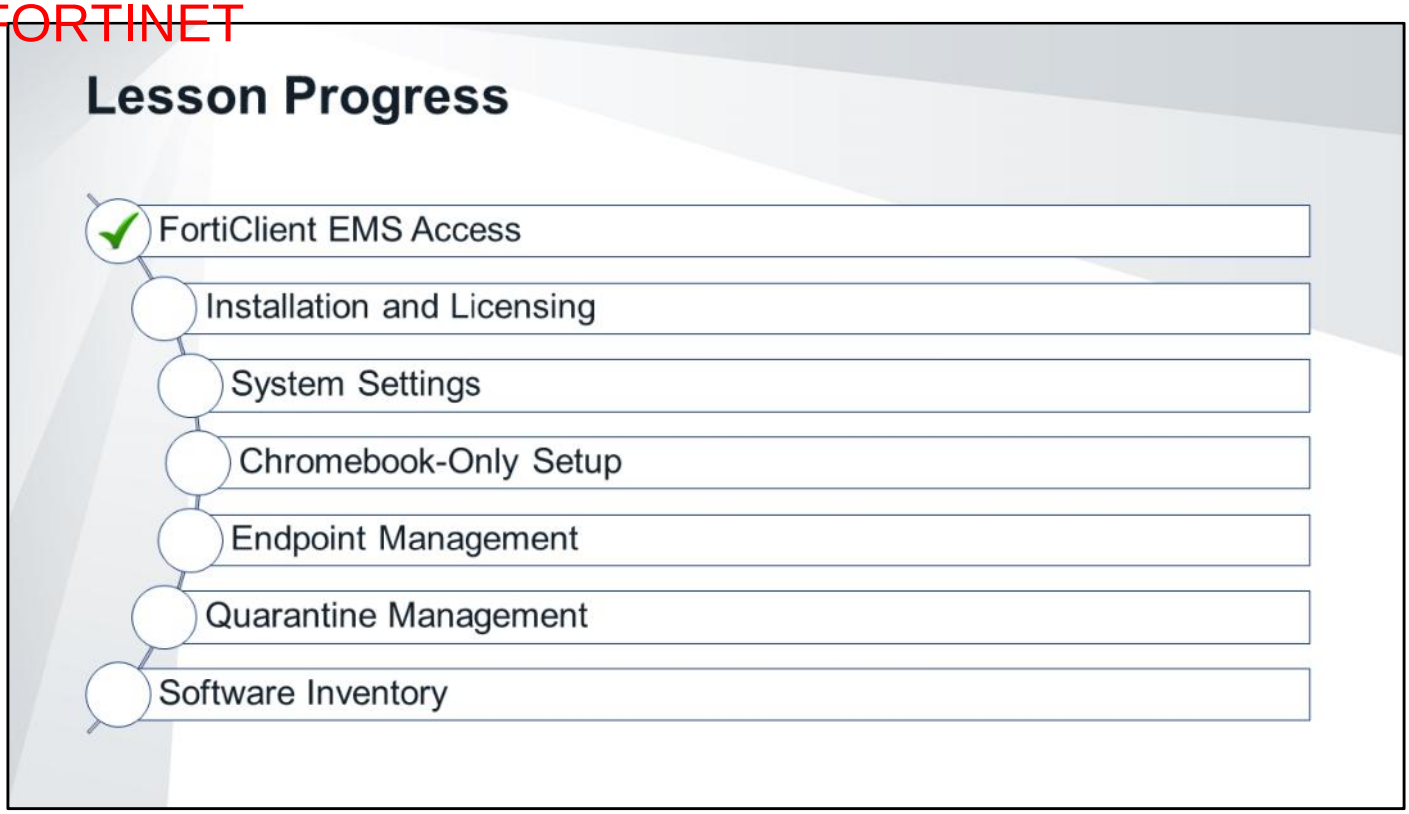
The FortiClient EMS dashboard provides a centralized summary of your system, endpoints, configuration, and summary information about vulnerability scans on endpoints.

The FortiClient Status dashboard includes a system Information widget and FortiClient status charts and widgets .

The Vulnerability Scan dashboard includes:
- Vulnerability scan charts and widgets
- Current vulnerabilities summary
- Endpoint scan status
- Top 10 vulnerable endpoints with high risk vulnerabilities

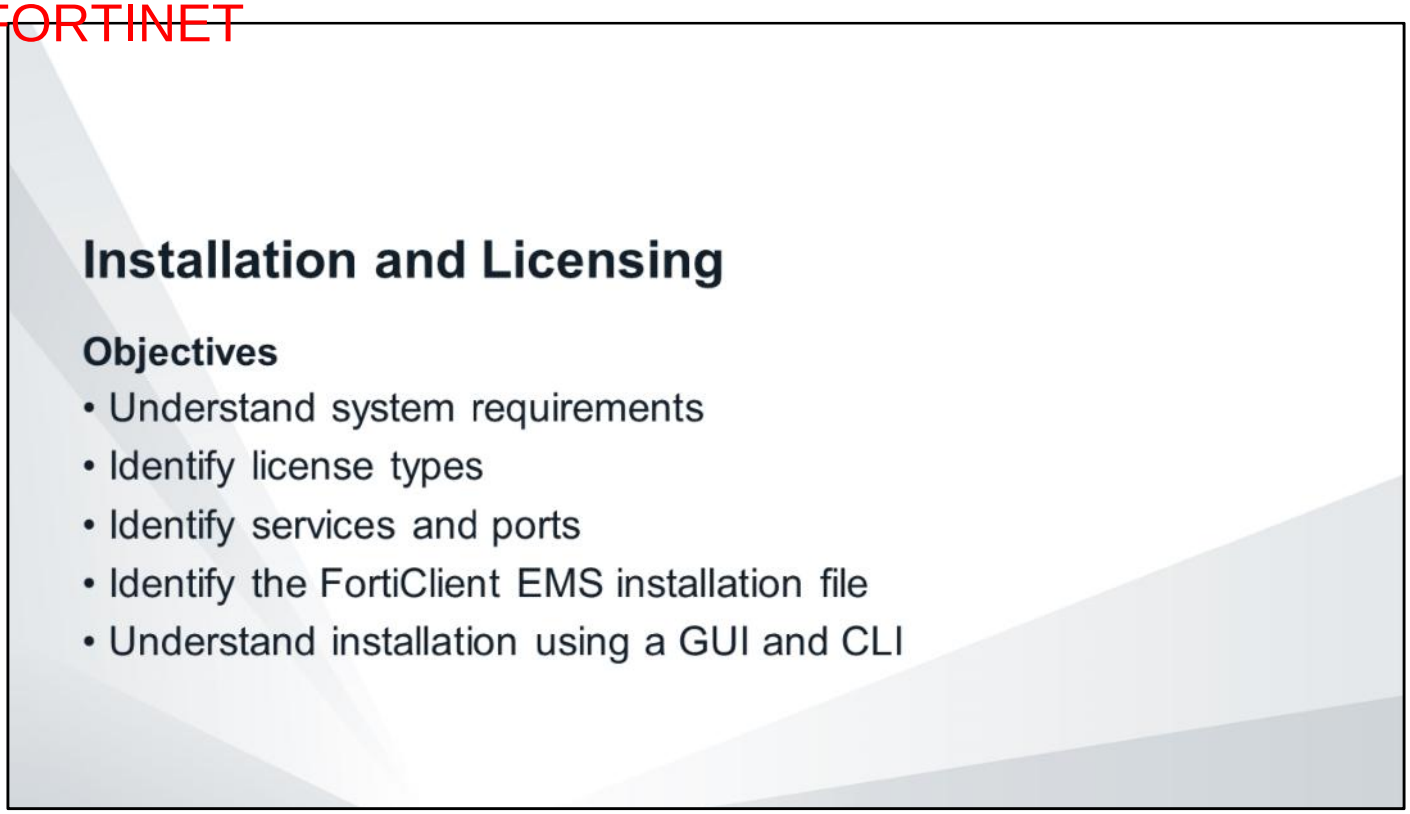
The dashboard also shows Chromebook status.





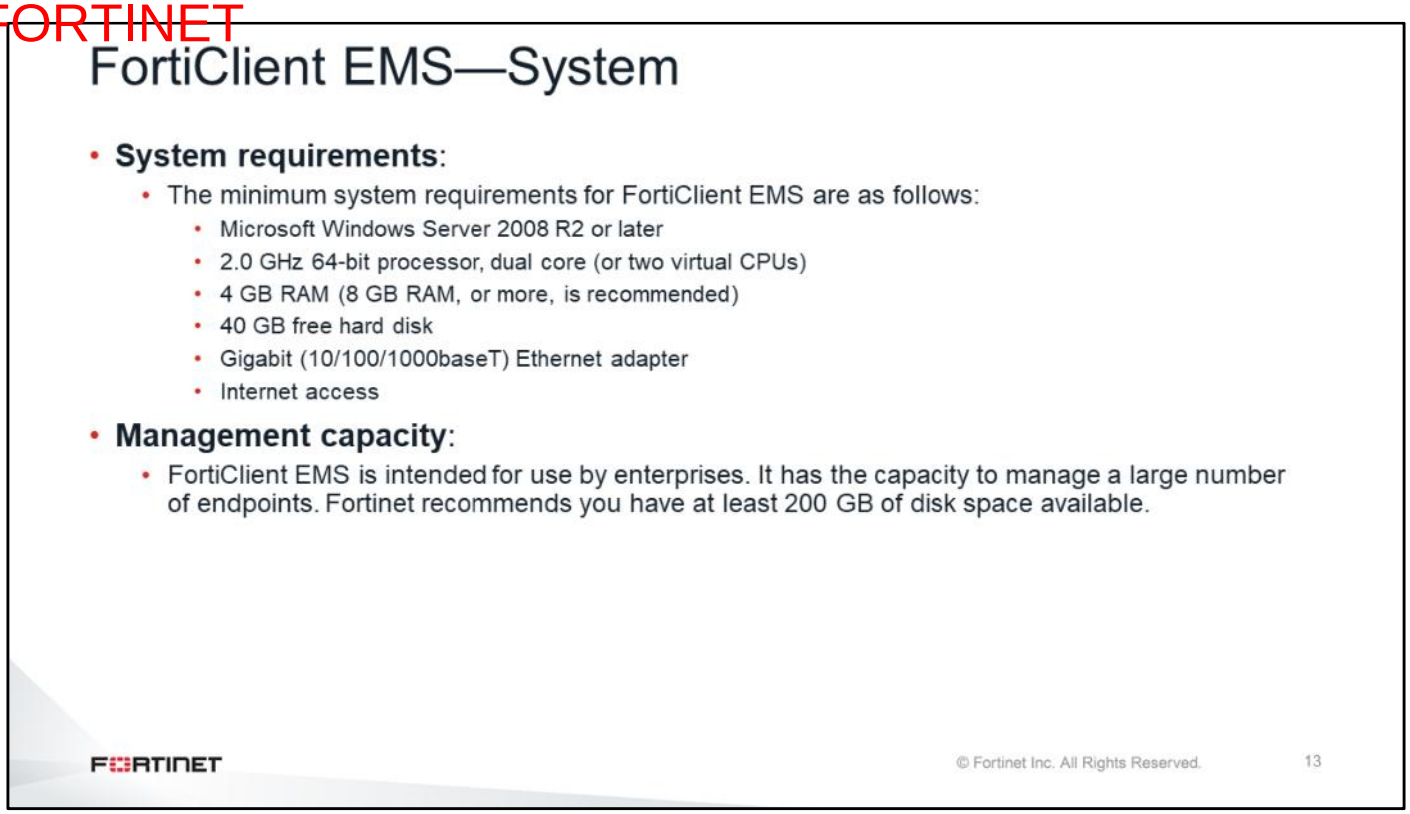
Good job! You now know how to access the FortiClientEMS GUI. You also learned about FortiClient EMS components, FortiClient administration, and database management.

Now, you will learn about system requirements, license types, service ports, and installation options for FortiClient EMS.



After completing this section, you should be able to achieve the objectives shown on this slide.

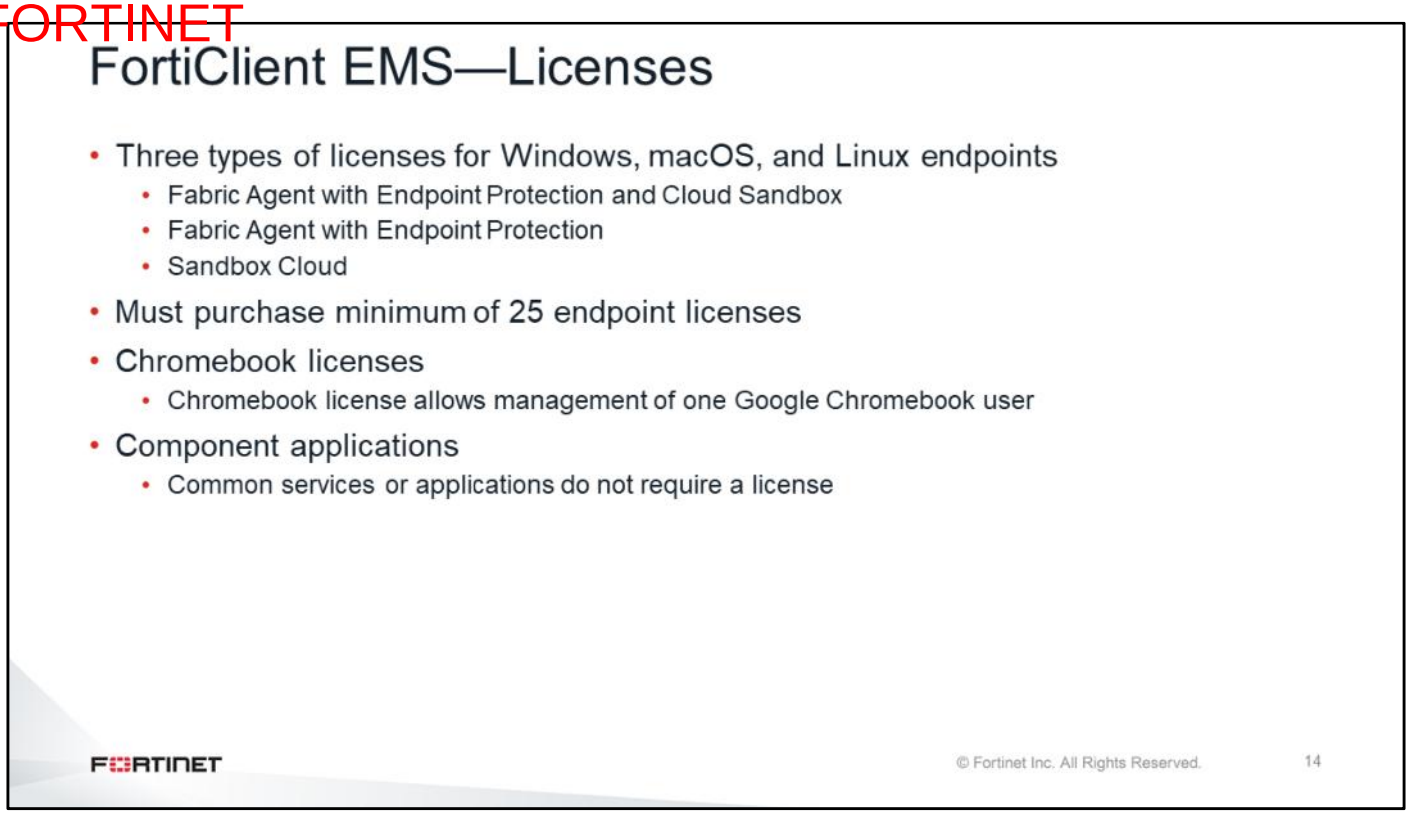
By demonstrating competence in installing and licensing FortiClient EMS, you will be able to understand system requirements, and identify license types, services, and ports. You will also know how to use the FortiClient EMS installation file to install FortiClient EMS using the GUI and CLI.



You should read the *FortiClient EMS Release Notes* to become familiar with the relevant software components and other important information about the product.

Internet access is required during installation. This becomes optional after installation is complete. FortiClient EMS accesses the Internet to obtain information about FortiGuard engine and signature updates.

Note that you should install only EMS and the default services for the operating system on the server. You should not install additional services on the same server as FortiClient EMS.



There are three types of licenses for Windows, macOS, and Linux endpoints:

1. Fabric Agent with Endpoint Protection and Cloud Sandbox is a full license that offers all FortiClient features including endpoint protection and Sandbox Cloud. This license includes all features detailed below for the Fabric Agent with Endpoint Protection and Sandbox Cloud licenses.
2. Fabric Agent with Endpoint Protection license includes support for telemetry and endpoint protection and management (AV, on-premise FortiSandbox, web filter, application firewall, vulnerability scan, FSSO, and FortiGate registration).
3. Sandbox Cloud license adds support for FortiSandbox Cloud for Windows endpoints.

Each purchased Fabric Agent license allows management of one FortiClient Windows, macOS, or Linux endpoint. You must purchase a minimum of 25 endpoint licenses, and you can have these EMS licenses for a maximum three year term. You can specify the number of endpoints and the term duration at time of purchase. Note that the Fabric Agent license also applies to iOS and Android endpoints.

A Chromebook license allows management of one Google Chromebook user. You must purchase a minimum of 25 Google Chromebook user licenses.

FortiClient EMS uses one license seat per logged-in user. If the user logs out, the license seat times out (default timeout value is `30` days), and the license is released. At this point, another user can use this license seat.

FortiClient EMS—Services and Ports

- You must enable the required ports and services for use by FortiClient EMS, and its associated applications, on your server

Communication	Usage	Protocol	Port	Incoming/Outgoing	How to customize
FortiClient Telemetry	FortiClient endpoint management	TCP	8013 (default)	Incoming	Installer/GUI
Samba (SMB) service	FortiClient EMS uses the SMB service during FortiClient initial deployment.	TCP	445	Outgoing	N/A
Distributed Computing Environment / Remote Procedure Calls(DCE/RPC)	The FortiClient EMS server connects to endpoints using RPC for FortiClient initial deployment.	TCP	135	Outgoing	N/A
AD server connection	Retrieving workstation and user information	TCP	389 (LDAP) or 636(LDAPS)	Outgoing	GUI
FortiClient download	Downloading FortiClient deployment packages created by FortiClient EMS	TCP	10443 (default)	Incoming	Installer
Apache/HTTPS	Web access to FortiClient EMS	TCP	443	Incoming	Installer
FortiGuard	FortiGuard AV, vulnerability, and application version updates	TCP	80	Outgoing	N/A
SMTP server/email	Alerts for FortiClient EMS and endpoint events. When an alert is triggered, EMS sends an email notification.	TCP	25 (default)	Outgoing	GUI
FortiClient endpoint probing	FortiClient EMS uses ICMP for endpoint probing during FortiClient initial deployment.	ICMP	N/A	Outgoing	N/A
FSSO	Connection to FortiOS.	TCP	8000	Incoming	N/A

FORTINET

15

The table on this slide shows the required ports and services that are required by FortiClient EMS to communicate with endpoints and servers running associated applications. You do not need to enable port 8013 and port 10443 on the server because the FortiClient EMS installation opens these.

FortiClient EMS—Services and Ports (Contd)

- FortiClient EMS services and ports to manage Chromebooks

Communication	Usage	Protocol	Port	Incoming/Outgoing	How to customize
The following ports and services only apply when using FortiClient EMS to manage Chromebooks:					
FortiClient on Chrome OS	Connecting to FortiClient EMS	TCP	8443 (default) You can customize this port.	Incoming	GUI
G suite API/Google Domain directory	Retrieving Google domain information using API calls	TCP	443	Outgoing	N/A
The following ports and services should be enabled for use on Chromebooks when using FortiClient for Chromebooks:					
FortiClient EMS	Connecting to the profile server	TCP	8443 (default)	Outgoing	Via Google Admin console when adding the profile
FortiGuard	Rating URLs	TCP	443, 3400	Outgoing	N/A
FortiAnalyzer	Sending logs to FortiAnalyzer	TCP	8443	Outgoing	N/A

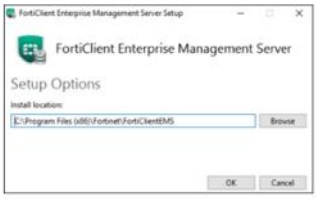
FORTINET

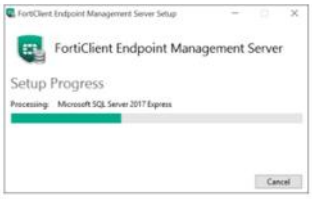
16

The table on this slide shows the required ports and services that are required by FortiClient EMS to communicate with Chromebook endpoints or Chromebook endpoints to communicate with FortiClient EMS.

FortiClient EMS—Installation File

- The installation file is available for download from the Fortinet Support website:
  - FortiClientEnterpriseManagement_6.2.X.<build>_x64.exe
- You can also receive the installation file from a sales representative
- FortiClient EMS installation package includes:
  - FortiClient EMS
  - Microsoft SQL Server 2017 Express Edition
  - Apache HTTP server



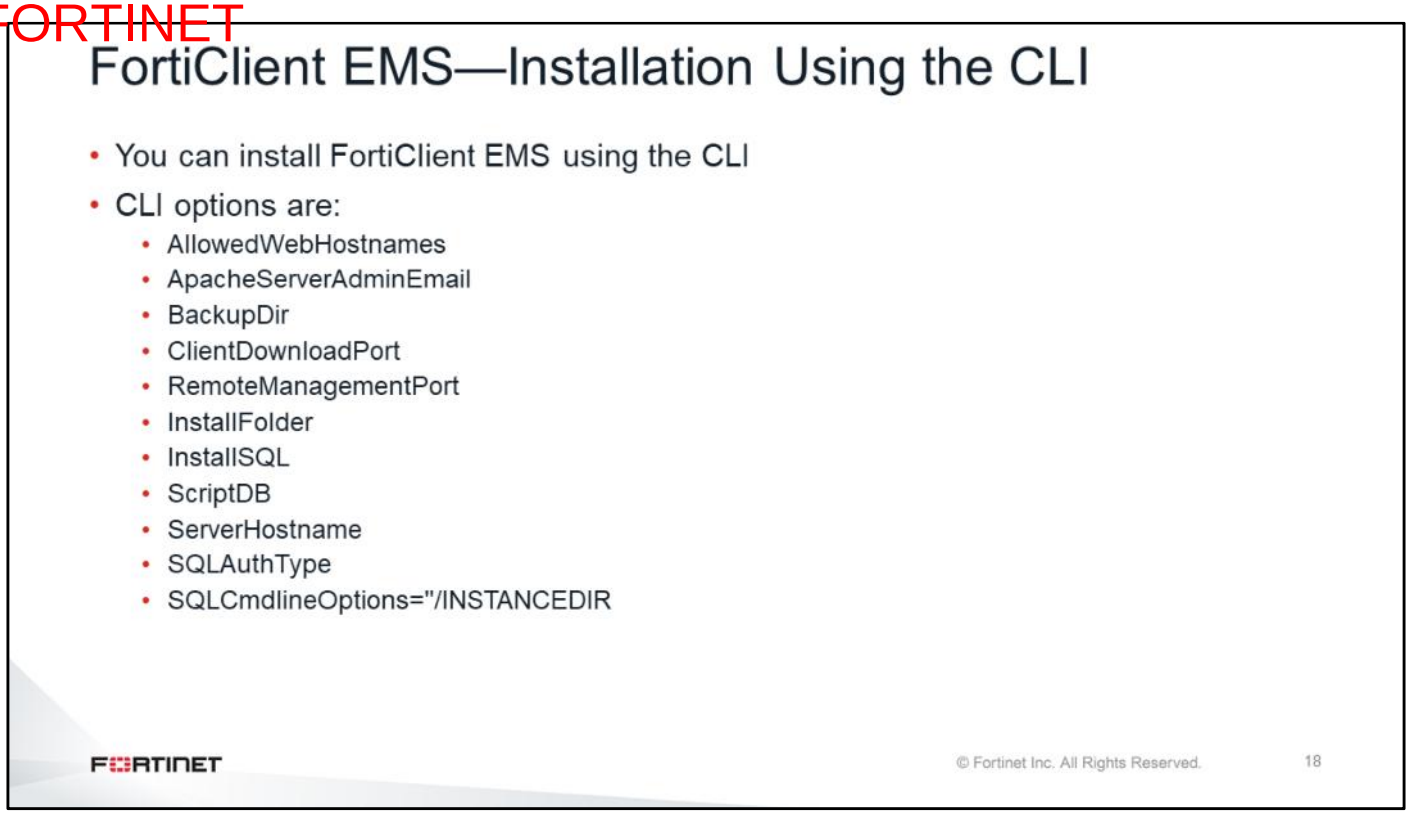


FORTINET

17

FortiClient EMS is available for download from the Fortinet Support website. You can also receive the installation file from a sales representative. The installation file available for FortiClient EMS is shown in this slide.

Note that local administrator rights and Internet access are required to install FortiClient EMS.

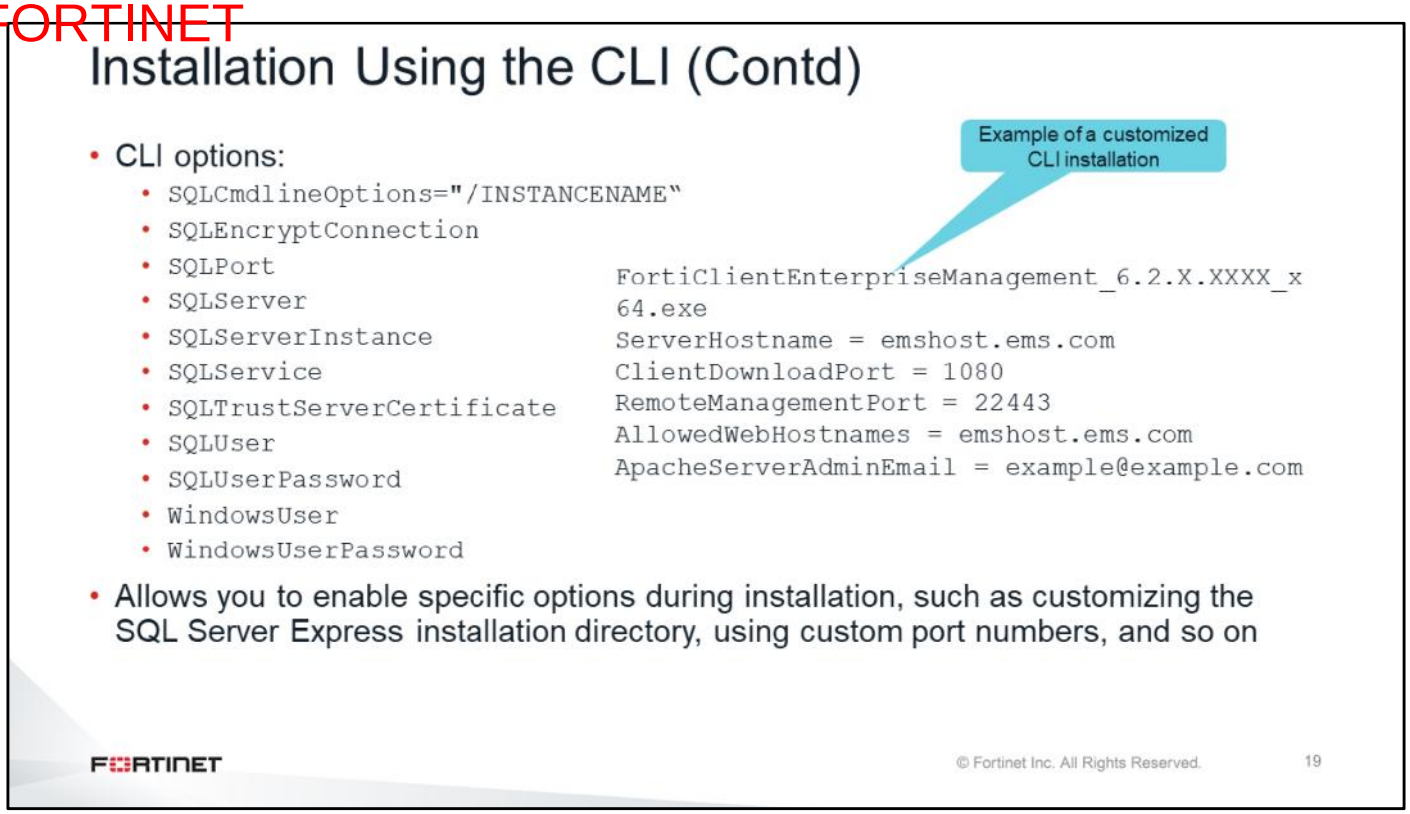


You can install FortiClient EMS using the CLI. The description of some CLI commands are as following:

The `AllowedWebHostnames` command allows you to configure the host name. The default value is localhost, `127.0.0.1`. To clear this value, first enter `AllowedWebHostnames=*`, then enter the desired `AllowedWebHostnames` value. Otherwise, the value entered will be appended to `localhost, 127.0.0.1`.

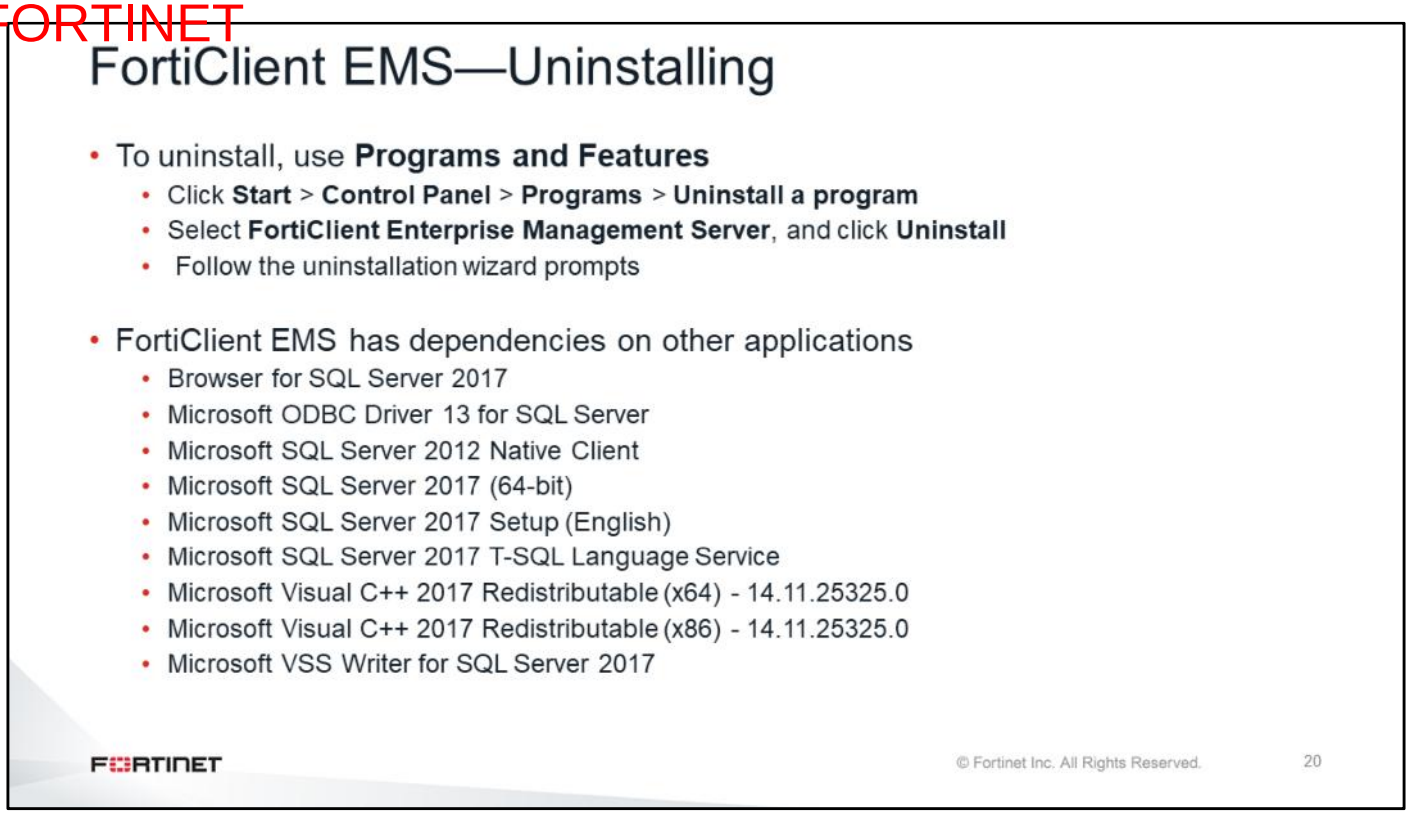
In `ApacheServerAdminEmail` option, you can configure the Apache server administrator's email address. By default, this is `admin@yourcompany.com`. The `BackupDir` option allows you to enter the desired backup directory path for the SQL server. Similarly, `ClientDownloadPort` allows you to enter the customized HTTP port number and `RemoteManagementPort` allows you to enter the HTTPS port number. The default values are 80 (HTTP) and 443.

For details on other CLI commands, refer to the *FortiClient EMS Administration Guide*.

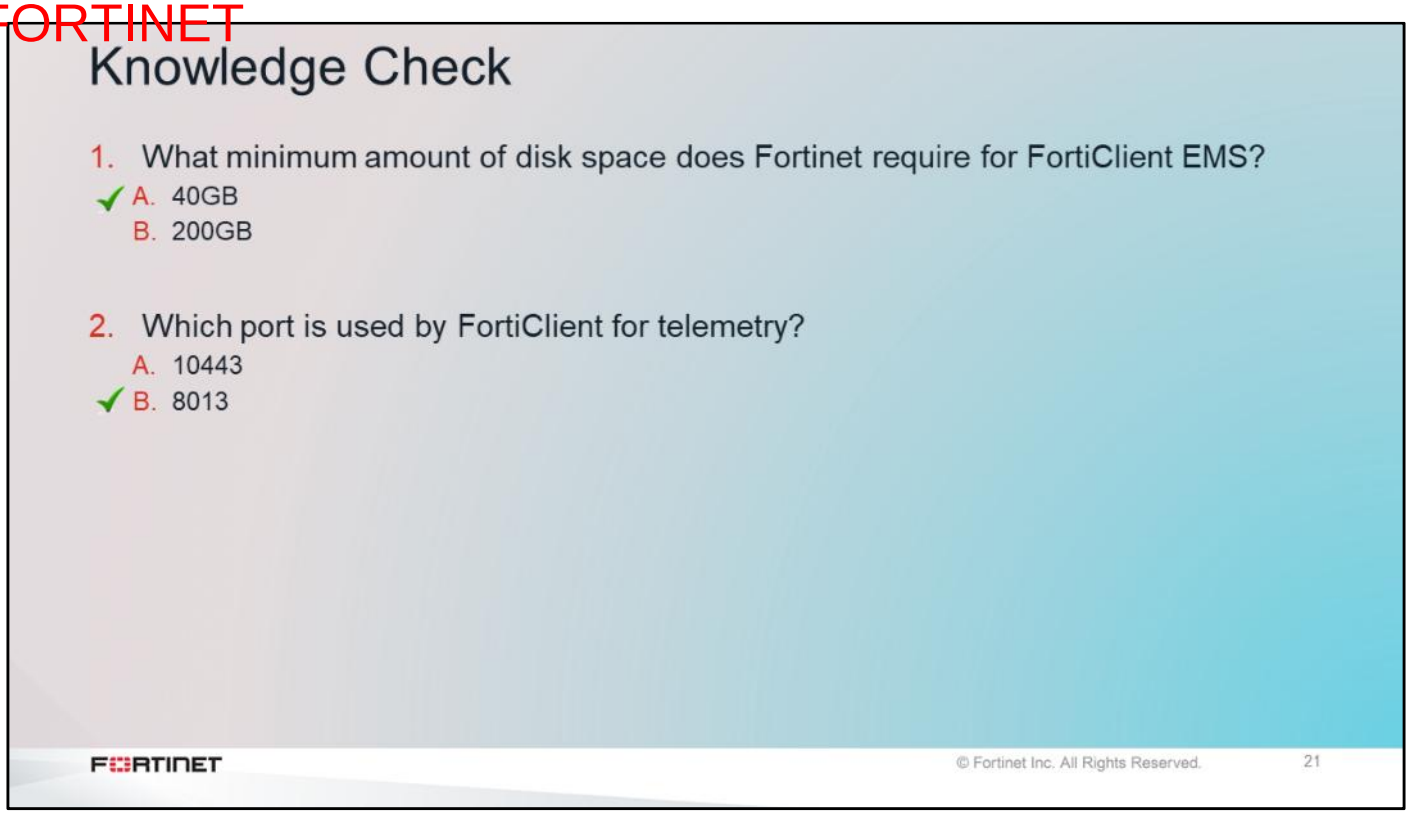


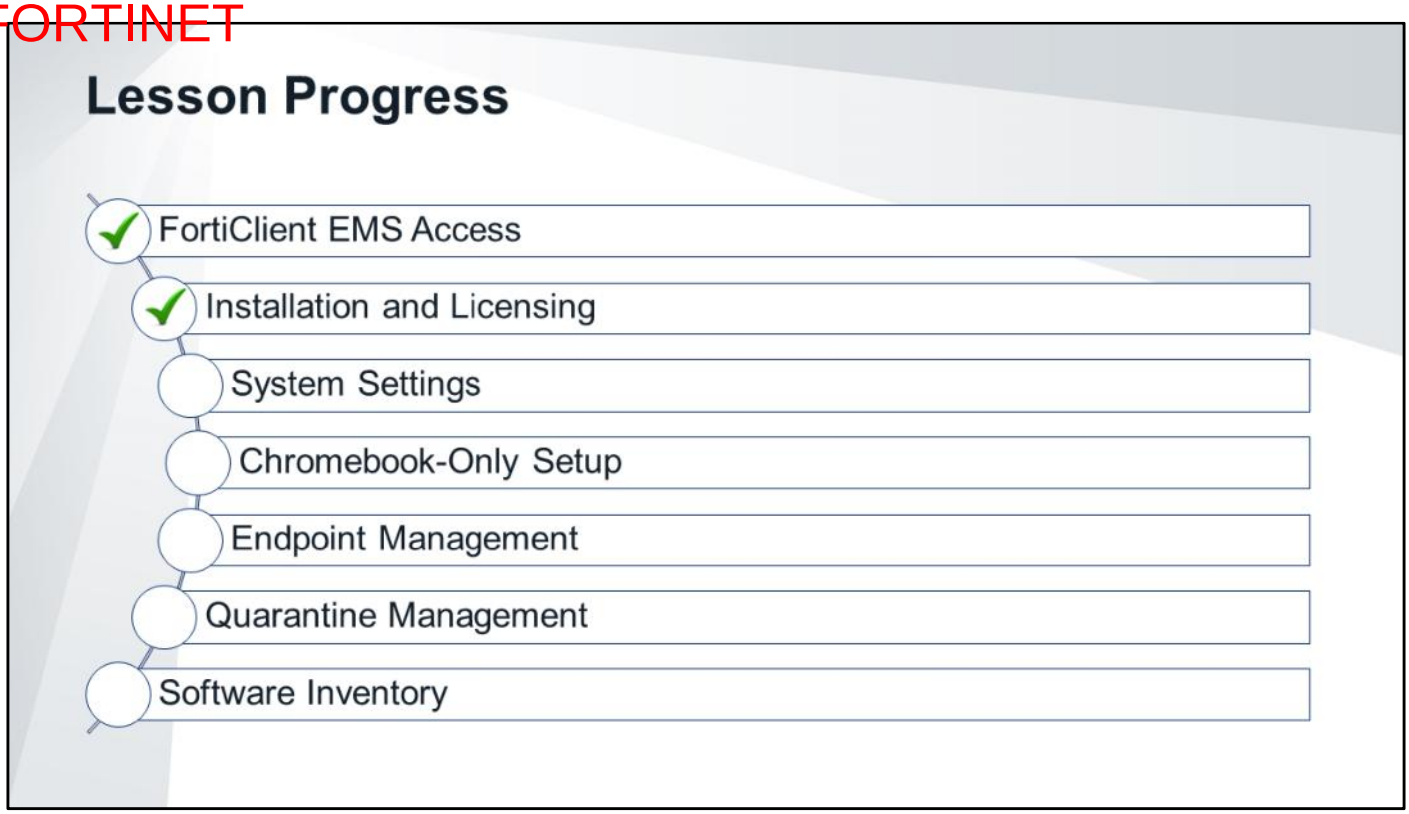
Installation using the CLI allows you to enable specific options during installation, such as customizing the SQL Server Express installation directory, using custom port numbers, and so on.

Take a look at the example of a customized configuration during CLI installation, on the slide.



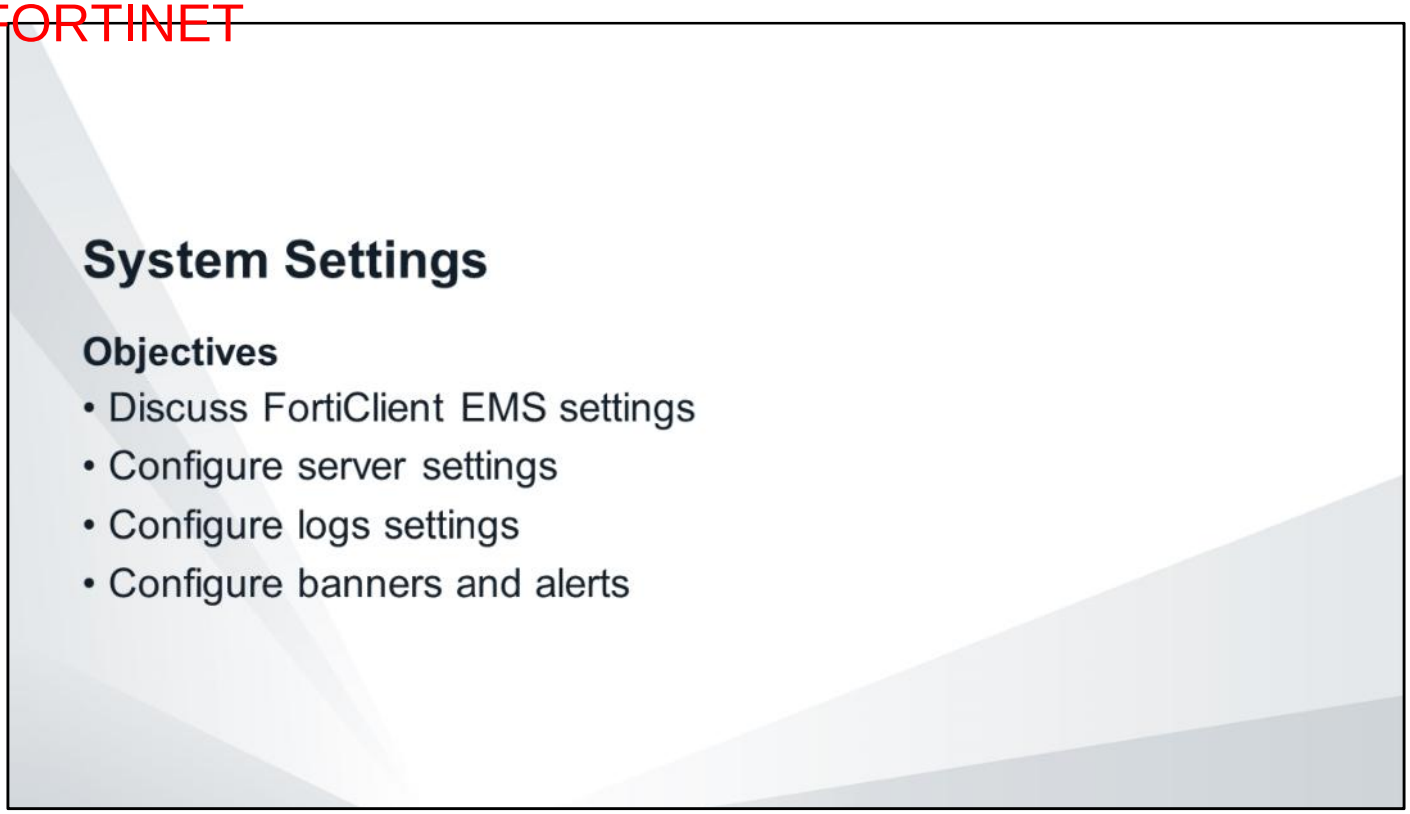
FortiClient EMS can be uninstalled using Windows **Add or Remove Program**. FortiClient EMS installs the dependencies. If other applications on the same computer are not using them, you can uninstall them manually, after removing FortiClient EMS. The list of dependencies are shown on this slide.





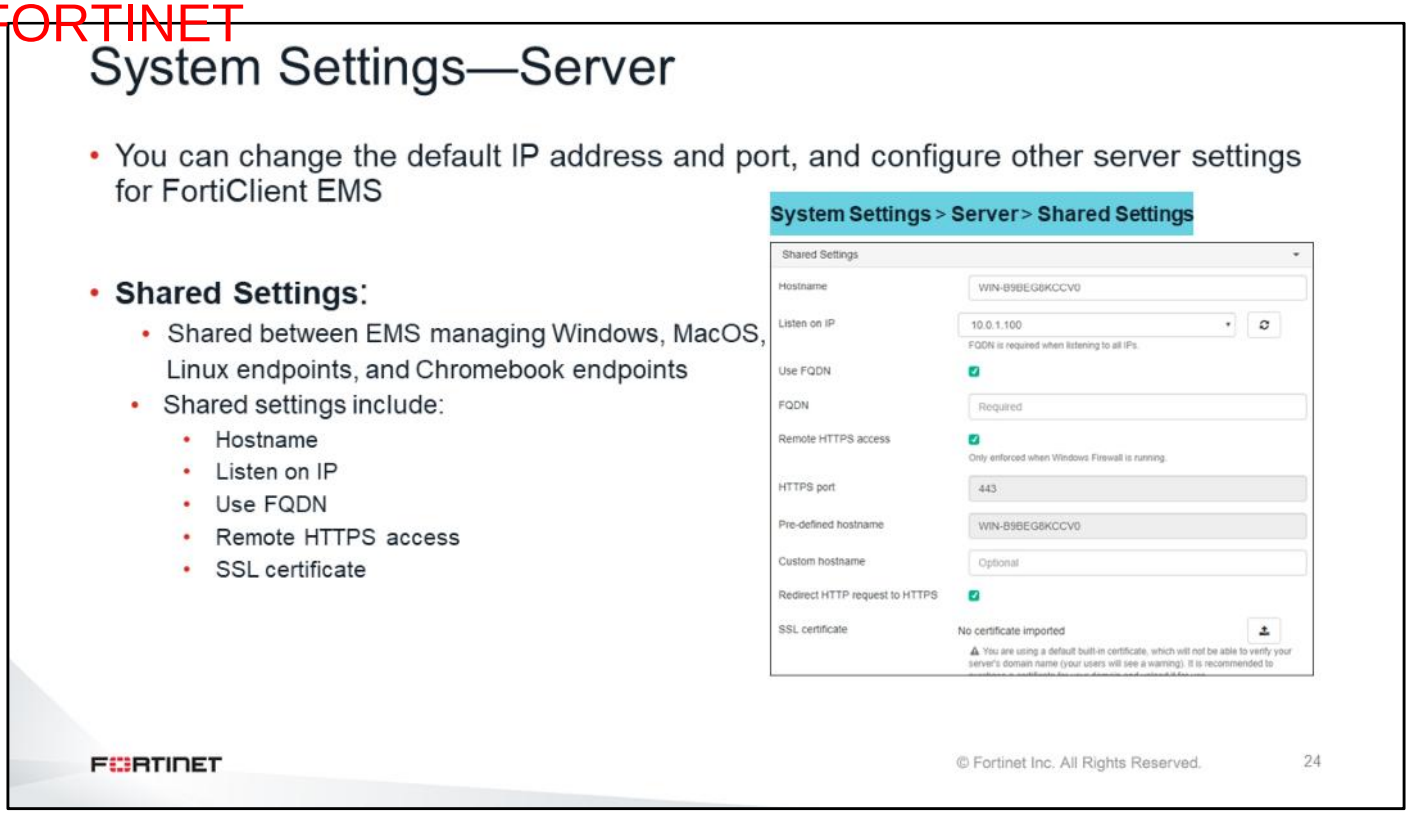
Good job! You now understand the system requirements to install FortiClient EMS. You also learned about license types, services, the FortiClient EMS installation file, as well as how to install FortiClient EMS using the GUI and CLI.

Now, you will learn about the FortiClient EMS system settings.



After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in FortiClient EMS system settings, you will be able to configure the server, logs, FortiGuard, endpoints, login banner, EMS alerts, endpoint alerts, SMTP server, and custom messages settings.

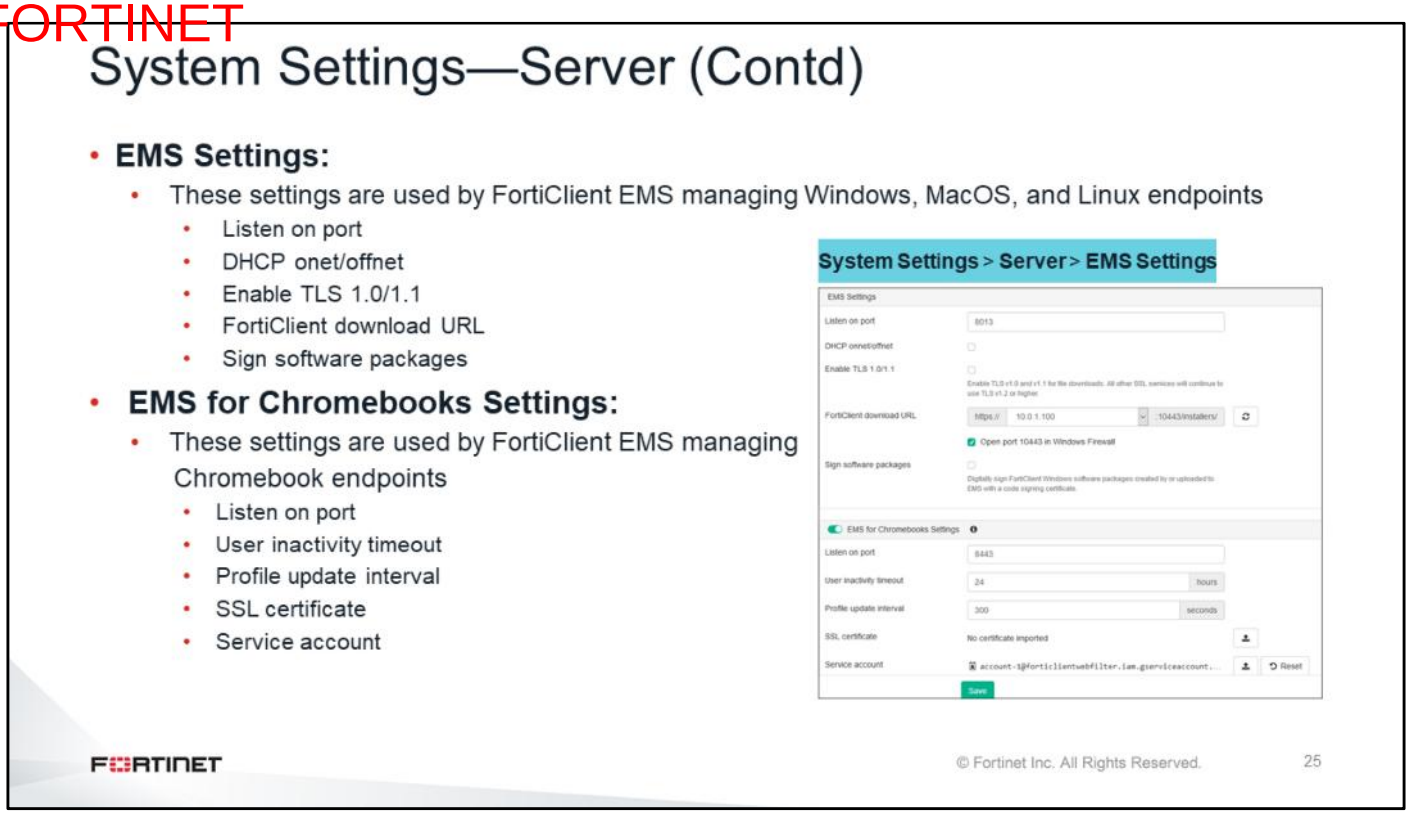


The FortiClient EMS **Shared Settings** option is shared between Windows, MacOS, Linux, and Chromebook endpoints. You can configure EMS hostname, IP address and FQDN. When you enable the **Use FQDN** option, FortiClient can connect using either the specified IP address in the **Listen on IP Addresses** field, or the specified FQDN.

The **Remote HTTPS access** option specifies settings for remote administration access to FortiClient EMS. You can enable or disable remote HTTPS access to FortiClient EMS. The following options are available when you select **Remote HTTPS access**:

- **HTTPS port** displays the HTTPS port configured on EMS. You can change to a new port. The default port is 443.
- **Pre-defined hostname** displays the NetBIOS name of the server at the installation that can not be changed .
- **Custom hostname** displays the host name of the server on which FortiClient EMS is installed. You can customize the host name. When you change the host name, the web server restarts.
- If you select **Redirect HTTP request to HTTPS**, and attempt to remotely access EMS using URL, this URL will automatically redirect to `https`.

The **SSL certificate** option displays the SSL certificate currently imported. If you have already uploaded an SSL certificate, the page displays the **Replace** button.



On the **EMS Settings** window, you can configure **Listen on port** setting by typing a new port number in the field. FortiClient will connect using the specified port. By default, it displays port 8013 for the FortiClient EMS server. Selecting **DHCP onnet/offnet** option, enables monitoring of endpoints within the company network (on-net). Endpoints that are connected to FortiClient EMS from outside the company network are off-net endpoints.

You can also enable or disable TLS 1.0 or 1.1 for file downloads. Windows 7 uses old TLS versions.

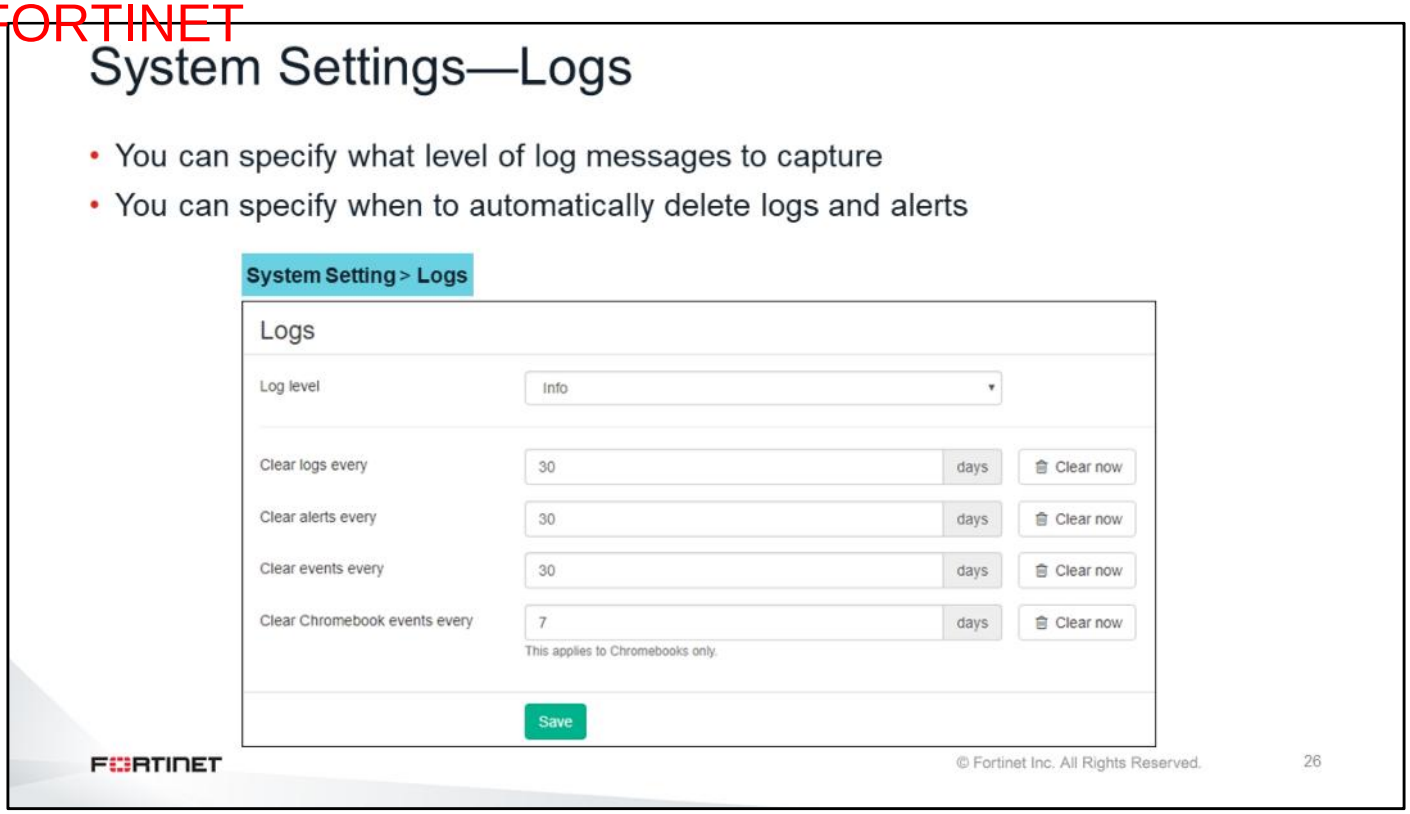
In the **FortiClient download URL** field you can see the URL on which FortiClient installers created on FortiClient EMS will be made available for download.

The **Sign software packages** option allows you to digitally signed Windows FortiClient software installers with a code signing certificate created by or uploaded to EMS.

The **EMS for Chromebooks Settings** also includes **Listen on port** which, like EMS settings, displays the default port for the FortiClient EMS server for Chromebooks. You can change the port by typing a new port number. The default port is 8443.

You can also configure the **User inactivity timeout** setting, which is the number of hours of inactivity after which the user is timed out. **Profile update interval** specifies the profile update interval, in seconds.

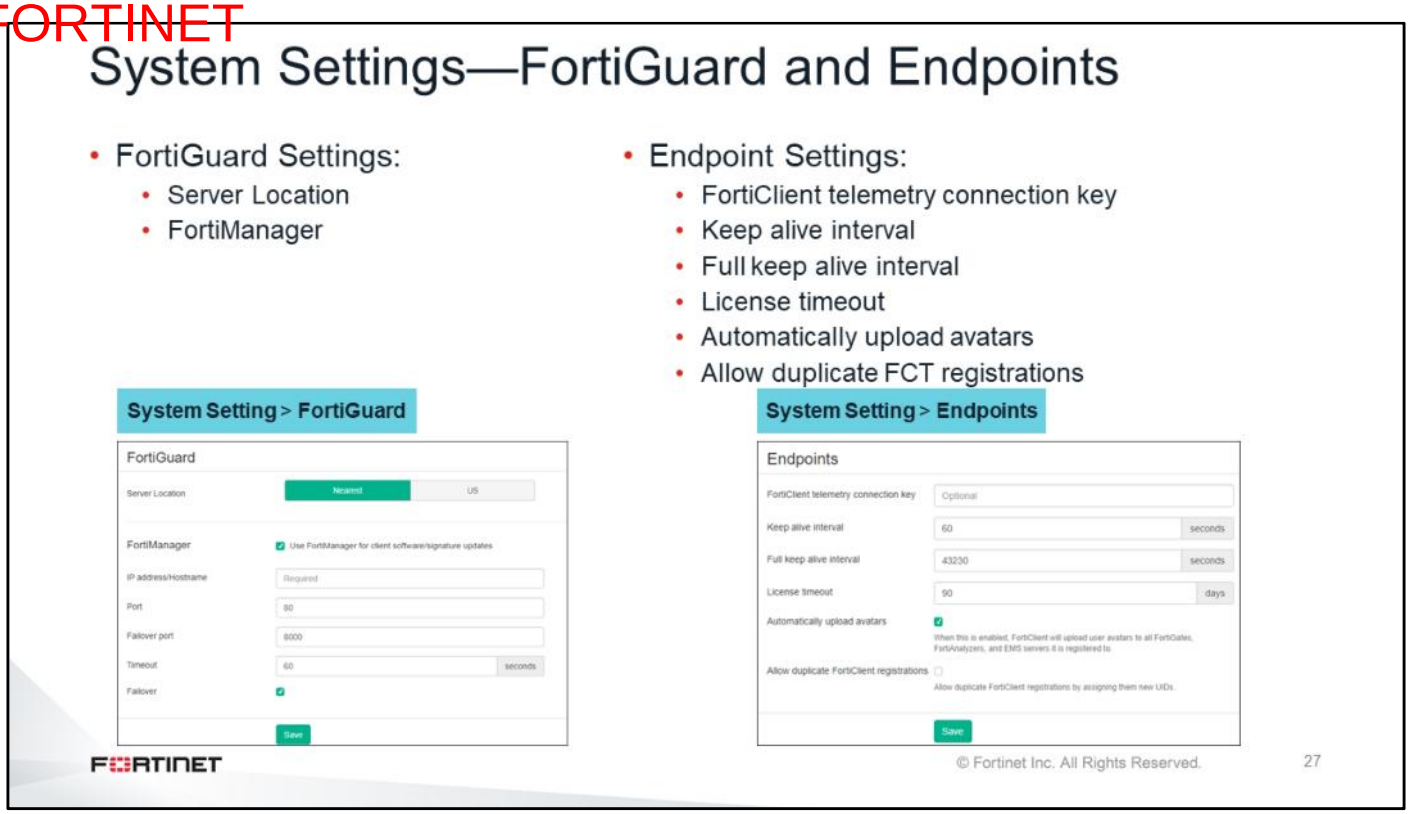
SSL certificate displays the SSL certificate currently imported. If you have already uploaded an SSL certificate, the page displays the **Replace** button. **Service account** displays the service account ID currently in use. You must enter an account ID and private key to update the account. Note that you must add an SSL certificate to FortiClient EMS to allow Chromebooks to connect to EMS.



In **Logs** section, you can specify what level of log messages to capture in the logs for FortiClient EMS. For example, if you select **Info**, all log messages from **Info** to **Emergency** are added to the FortiClient EMS logs.

You can also specify when to automatically delete logs, alerts, and events. By default, it is `30` days for all logs, alerts, and other OS events, and `7` days for Chromebook events.

You can click **Clear now** to immediately delete all FortiClient EMS logs, alert, or events.



The FortiGuard settings include **Server Location**, which allows you to configure the FortiGuard server location to **Nearest** or **US**.

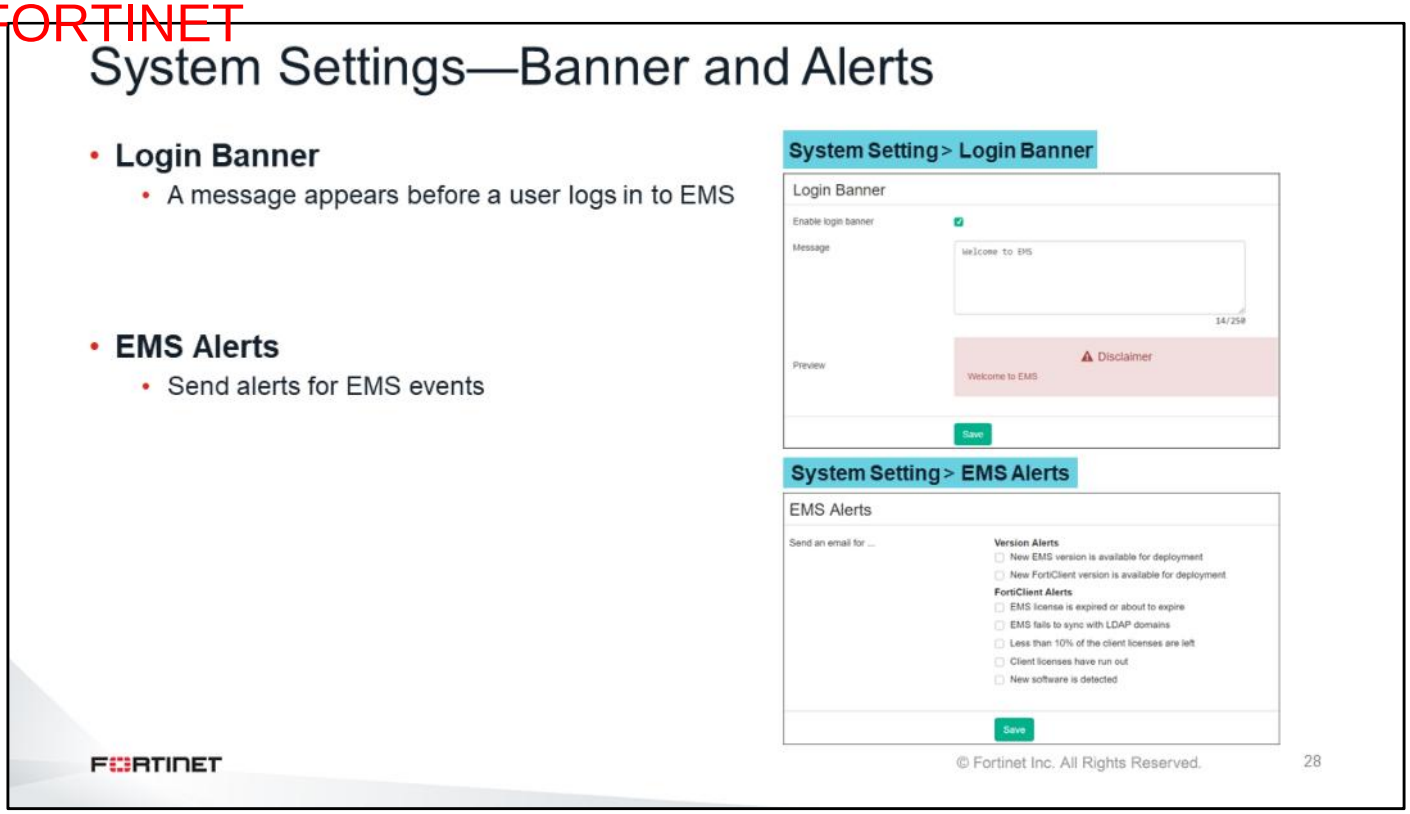
- If you select **Nearest**, FortiClient EMS connects to the FortiGuard server whose IP address is provided by the DNS server.
- If you select **US**, FortiClient EMS can connect only to FortiGuard servers available in the United States and does not attempt to access a FortiGuard server outside the US.

You can also configure the **FortiManager** option, which allows you to use FortiManager for client software and signature updates. If you select **Failover**, this enables failover to FDN, when FortiManager for FortiClient is not available. The settings in the Endpoints window allows you to add the FortiClient telemetry connection key for FortiClient EMS. FortiClient must provide this key during connection. You can also configure keep alive intervals. FortiClient sends short and full keep alive messages to FortiClient EMS at the specified intervals.

When FortiClient endpoint is registered to EMS, it consumes a license seat. You can configure a license timeout value in days.

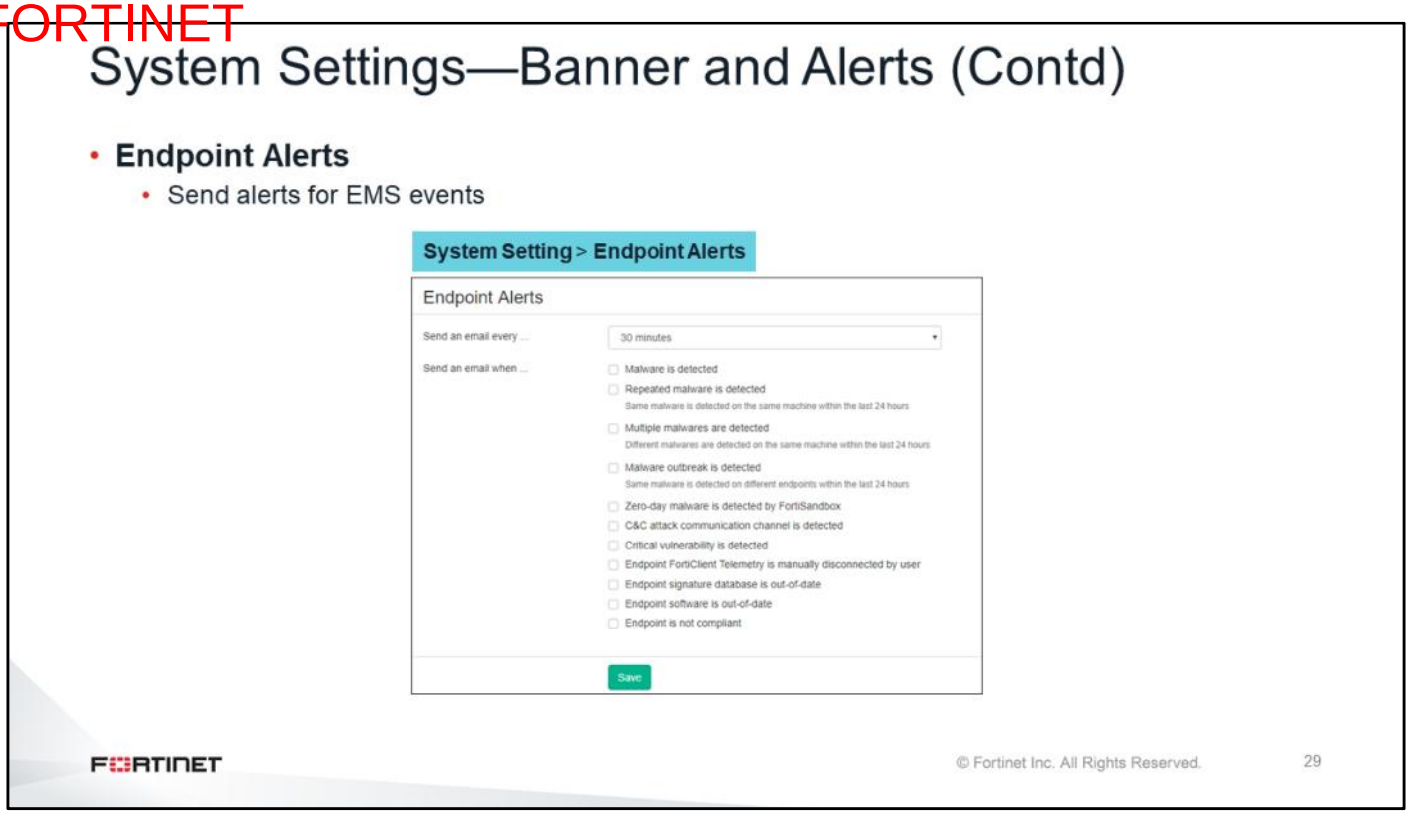
- If an endpoint disconnects from EMS, the license seat is retained in anticipation that the endpoint will reconnect. If the endpoint does not reconnect within the given time out, its connection record is removed from EMS.
- If the endpoint is removed, switched off, or goes offline, and does not re-establish a telemetry connection to EMS within the given time out, the endpoint is deleted from EMS even if FortiClient on the endpoint shows that it is still connected.

The **Automatically upload avatars** option allows FortiClient to uploads user avatars to all of the devices and the **Allow duplicate FCT registrations** setting allows duplicate FortiClient registrations by assigning the duplicate registrations new UIDs.

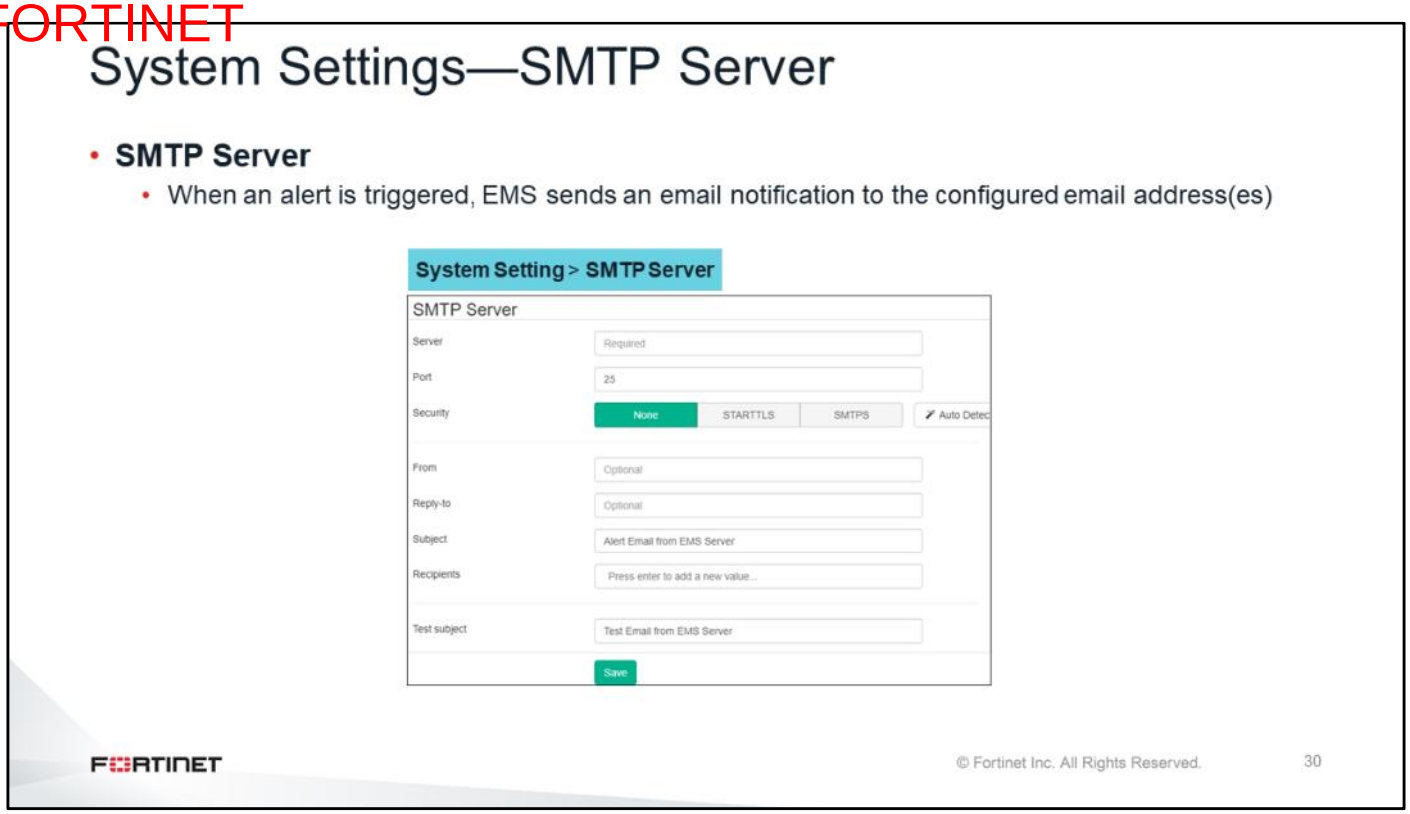


When you select the **Enable login banner** check box, a message appears on the login screen before a user logs in to EMS as shown in this slide. When you type a message and save in the **System Settings** > **Login Banner**, the **Preview** section displays a preview of the message.

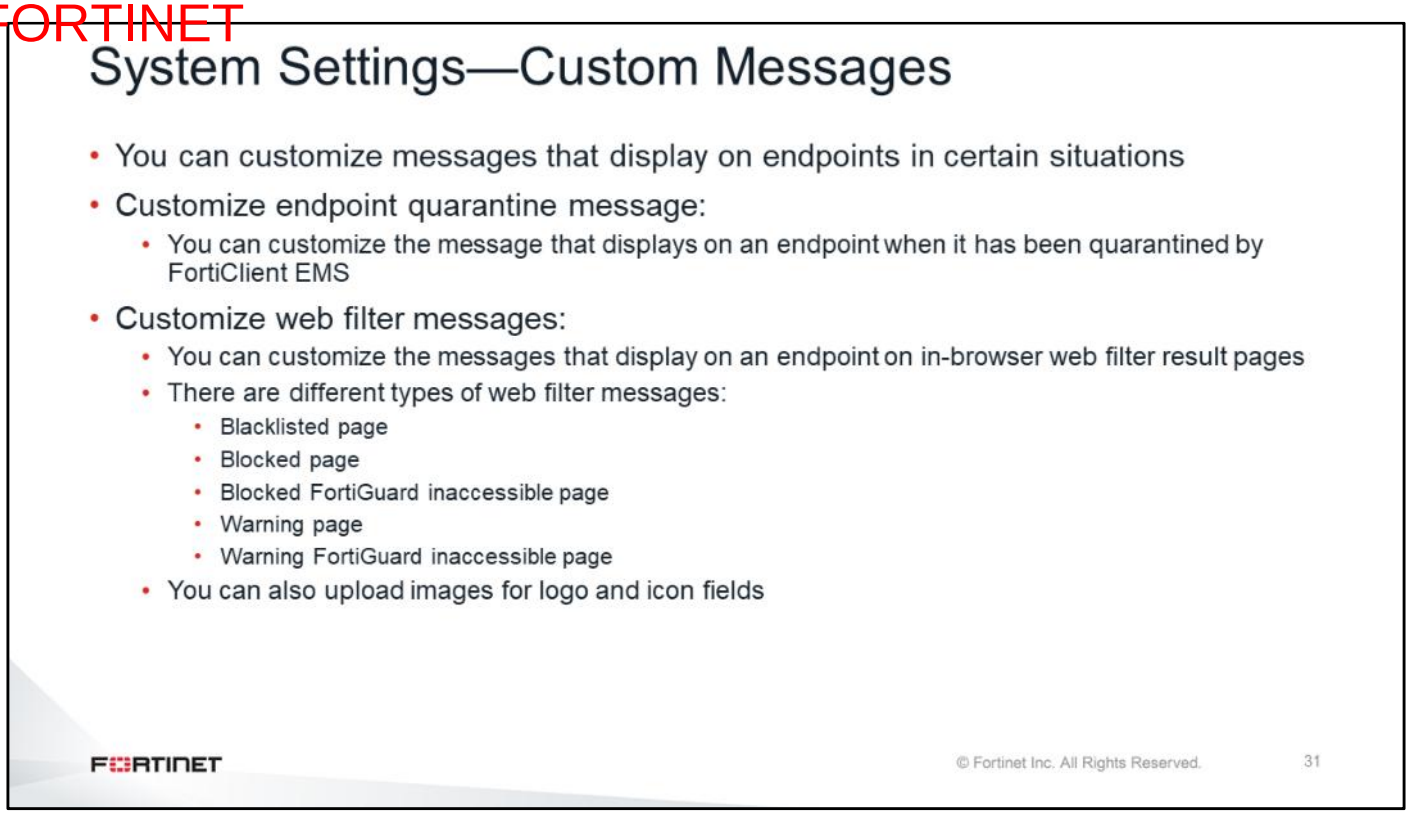
The **EMS Alerts** window allows you to send an email for version and FortiClient alerts. This slide shows all of the alerts that are available on the EMS Alerts window.



On the **Endpoint Alerts** window, you can enable the option to send an email alert for the endpoints. This slide shows all the endpoint events that you can select to generate email alerts. You can also select a time interval to send alert emails. By default, it is set to `30 minutes`.



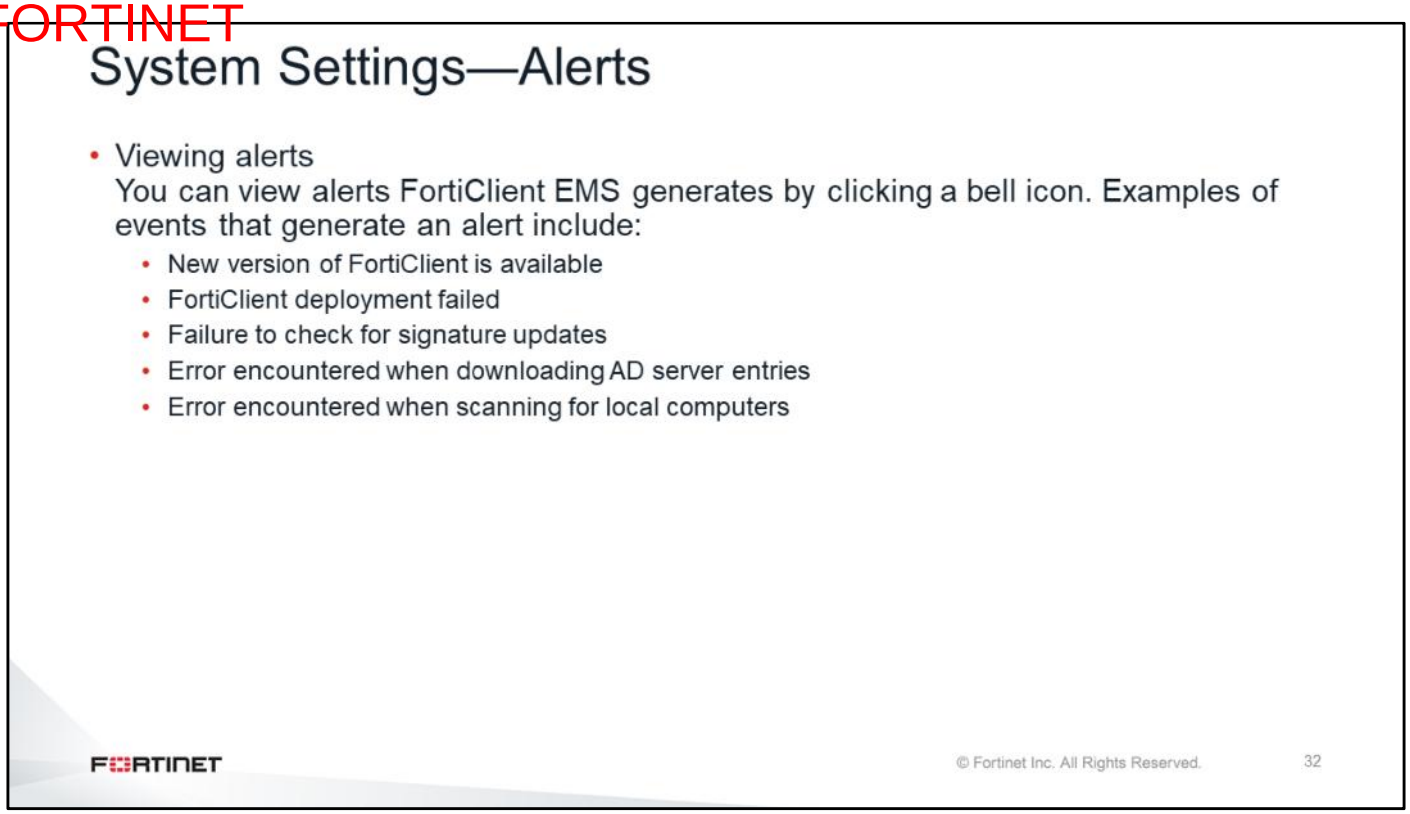
On the **SMTP Server** window, you can set up an SMTP server to enable alerts for EMS and endpoint events. All the options available for SMTP server configuration are shown in this slide. In the **Security** field, if you select **STARTTLS** or **SMTPS**, the **Username** and **Password** fields are enabled.



You can customize messages that display on endpoints in certain situations, such as when EMS has quarantined the endpoint. For example, you can customize the message to include your organization's help desk phone number so that users can contact the network administrator about their machine.

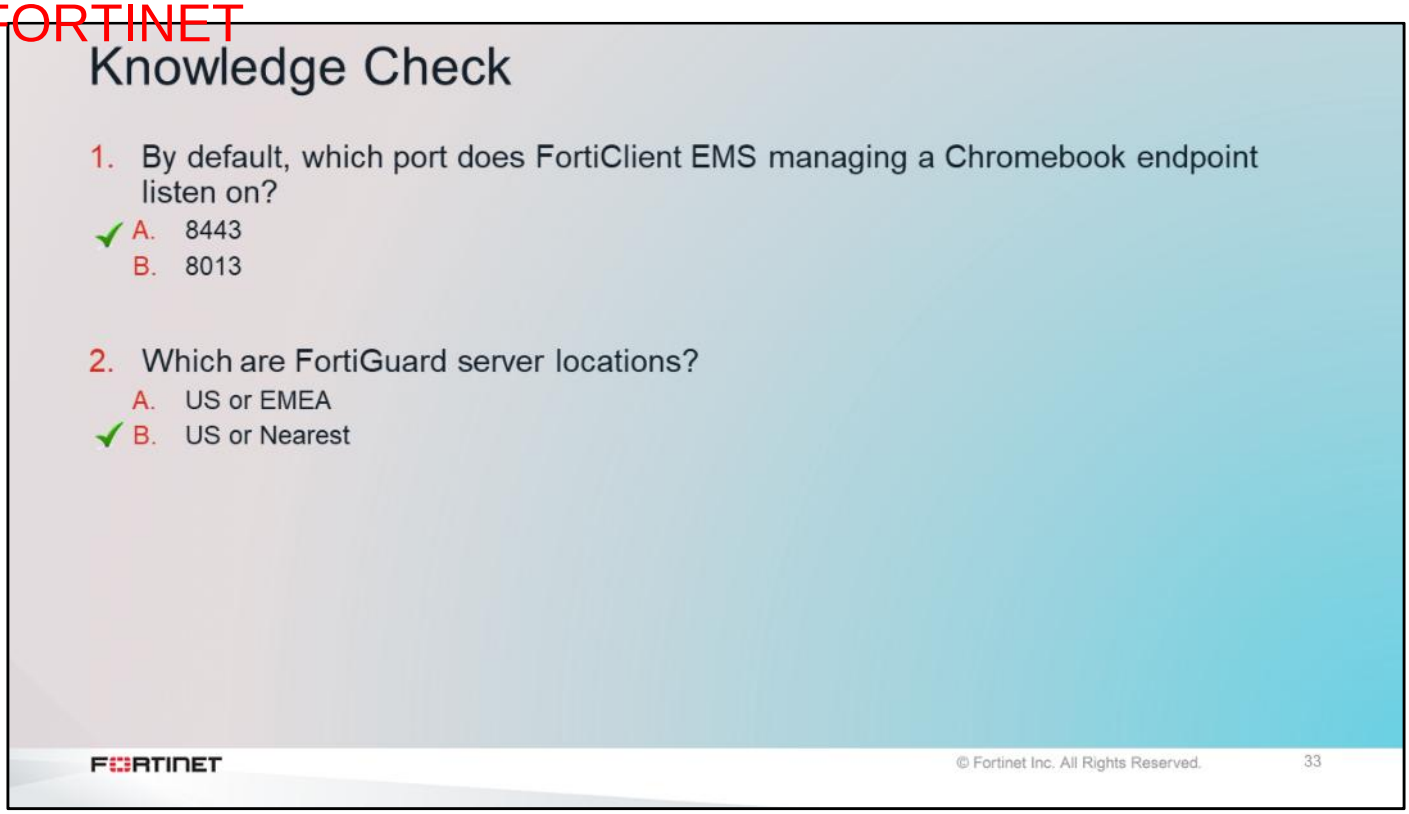
You can also customize the messages that display on an endpoint in in-browser web filter result pages. In **Custom Messages**, select **WebFilter Custom Messages**. The left panel displays the customization fields, while the right panel previews the custom messages as they will appear in a web browser when using the latest version of FortiClient. The types of web filter messages are: blacklisted page, blocked page, blocked FortiGuard inaccessible page, warning page, and warning FortiGuard inaccessible page.

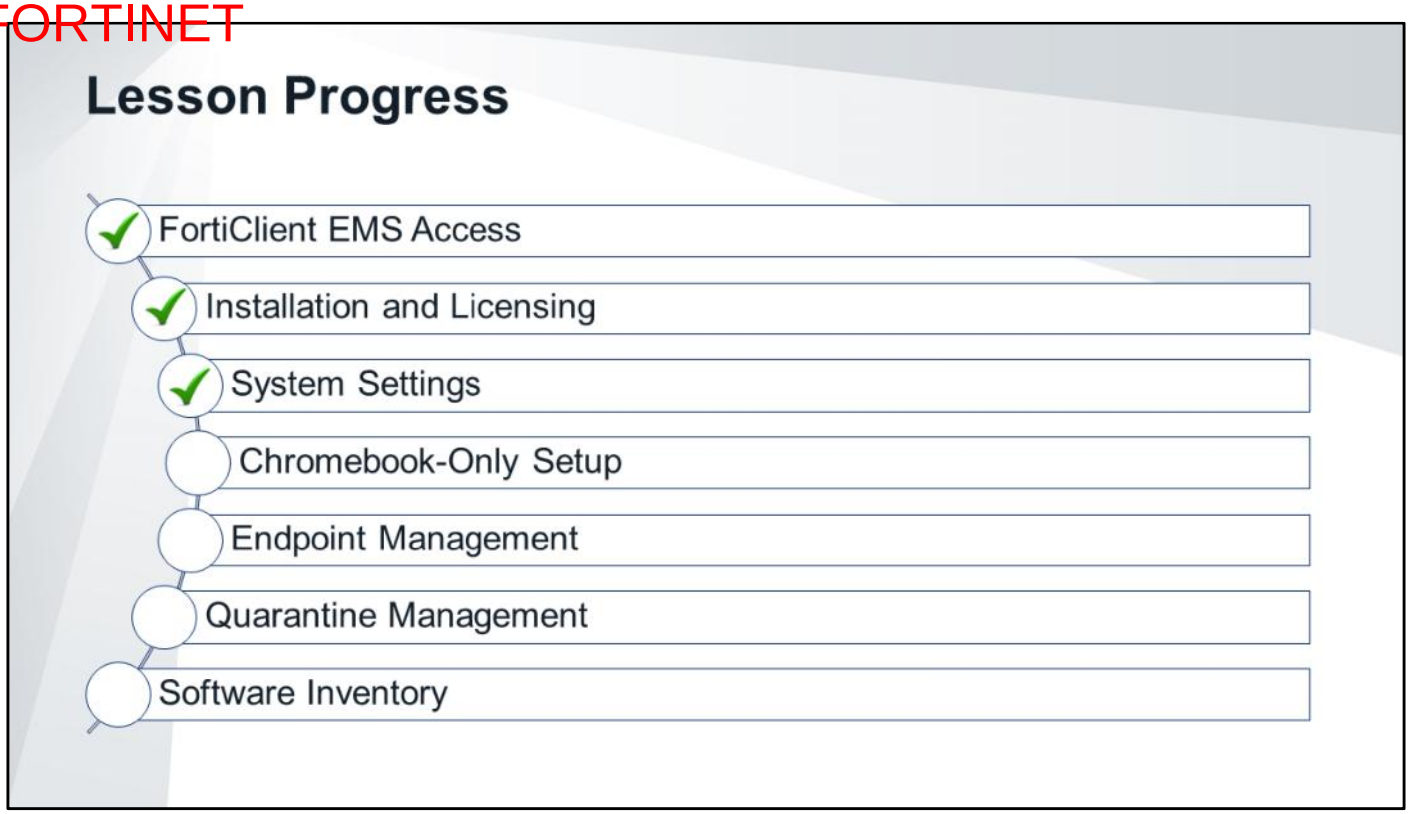
In the left pane, enable or disable the fields and enter the desired messages. You can also upload images for logo and icon fields. The right pane displays previews of the messages.



You can view the alerts FortiClient EMS generates. Examples of events that generate an alert are shown on this slide. A red label is associated with the **Alert** icon when new notifications are available or received. It is cleared when you view the alert.

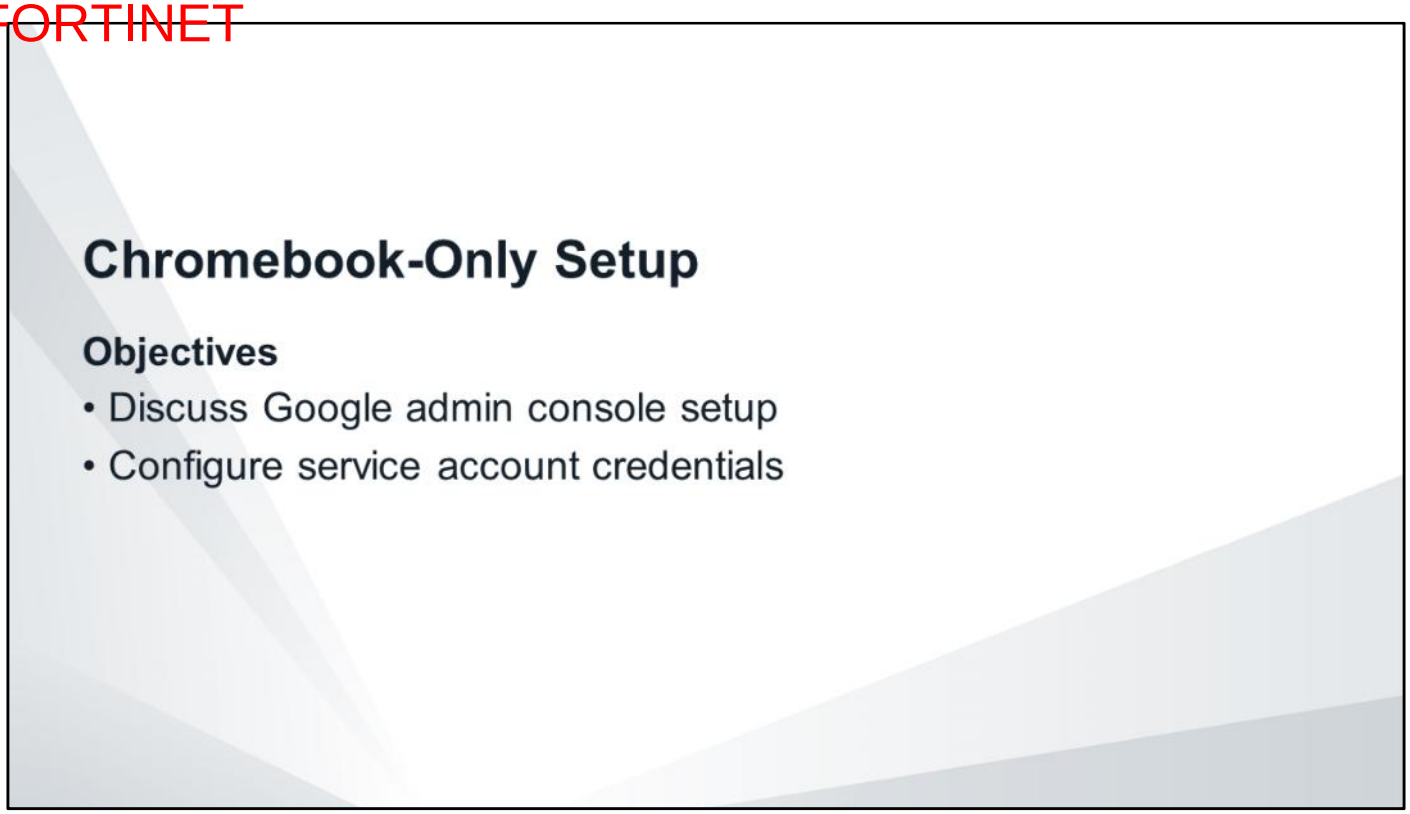
You select the **Alert** icon (a bell) in the toolbar to view alerts. You can use the **Filter** icon in each column heading to apply filters, and the **Clear Filters** icon to remove the filters





Good job! You now understand the system settings for FortiClient EMS.

Now, you will learn how to set up FortiClient EMS for Chromebook only.

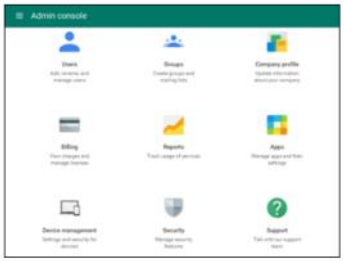


After completing this section, you should be able to achieve the objectives shown on this slide.

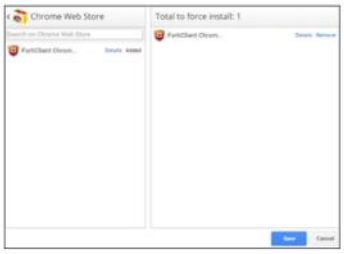
By demonstrating competence in setting up FortiClient EMS to manage Chromebooks, you will be able to configure the Google admin console setup and service account credentials.

Chromebook-Only Setup—Admin Console Setup

- Logging in to the Google Admin console



- FortiClient Web Filter extension
  - You must add extension ID `igbgpehnbmhgdgjbhkkpedommgmfbeao` to enable the web filter feature for Chromebook endpoints



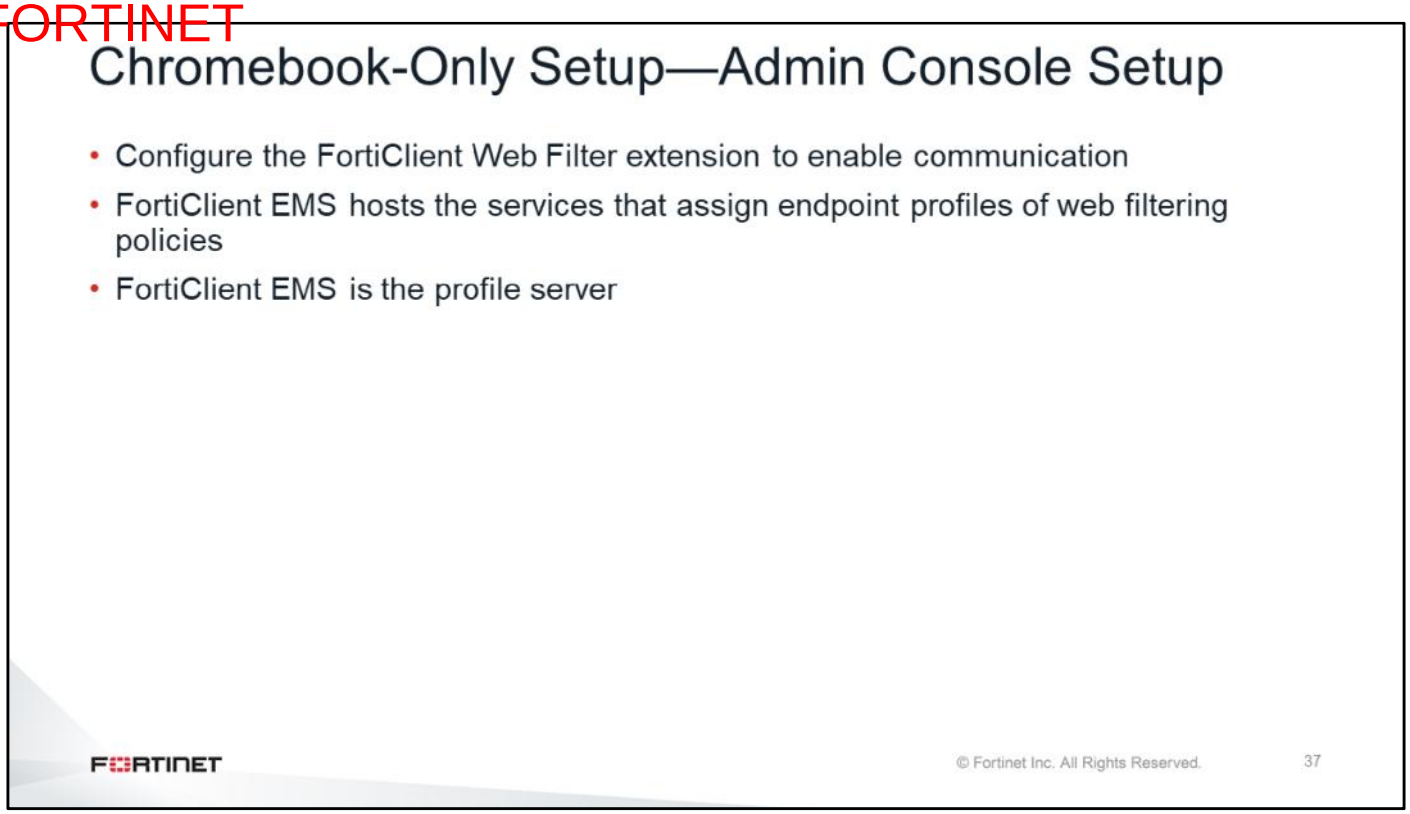
FORTINET

 36

Log in to the Google admin console using your Google domain admin or G Suite account. Note that a Google account set up through an organization like work, school, a club, or maybe family or friends, is called a G Suite account.

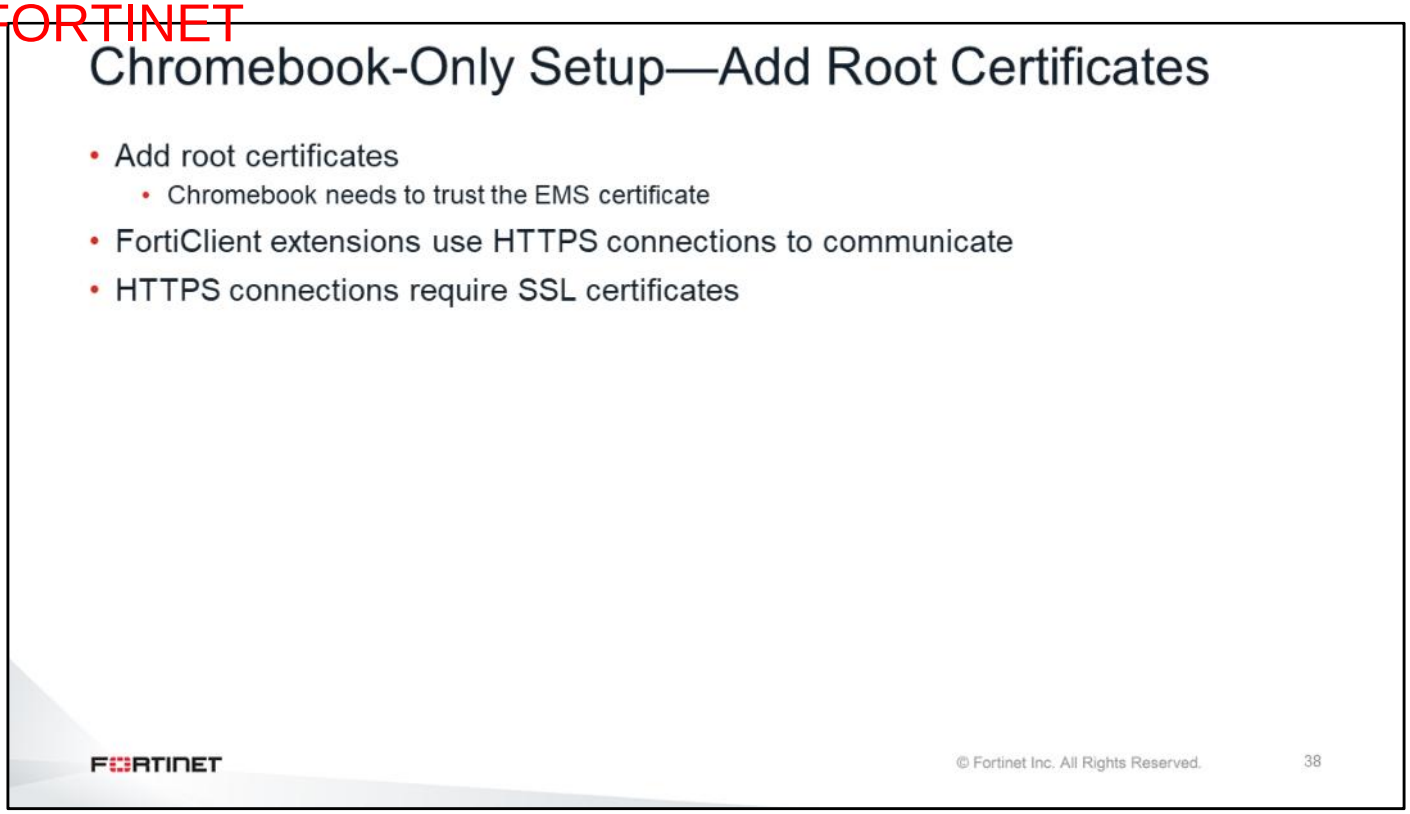
After the FortiClient Web Filter extension is added, on the **Chrome Web Store** window, search for the extension ID shown in this slide. The extension name appears as **FortiClient Chromebook Web Filter Extension**.

Note that FortiClient EMS software is not available for public use. You can enable the feature only by using the extension ID that is shown in this slide.



You must configure the FortiClient Chromebook Web Filter extension to enable the Google Admin console to communicate with FortiClient EMS. FortiClient EMS hosts the services that assign endpoint profiles of web filtering policies to groups in the Google domain. FortiClient EMS also handles the logs and web access statistics sent from the FortiClient web filter extensions.

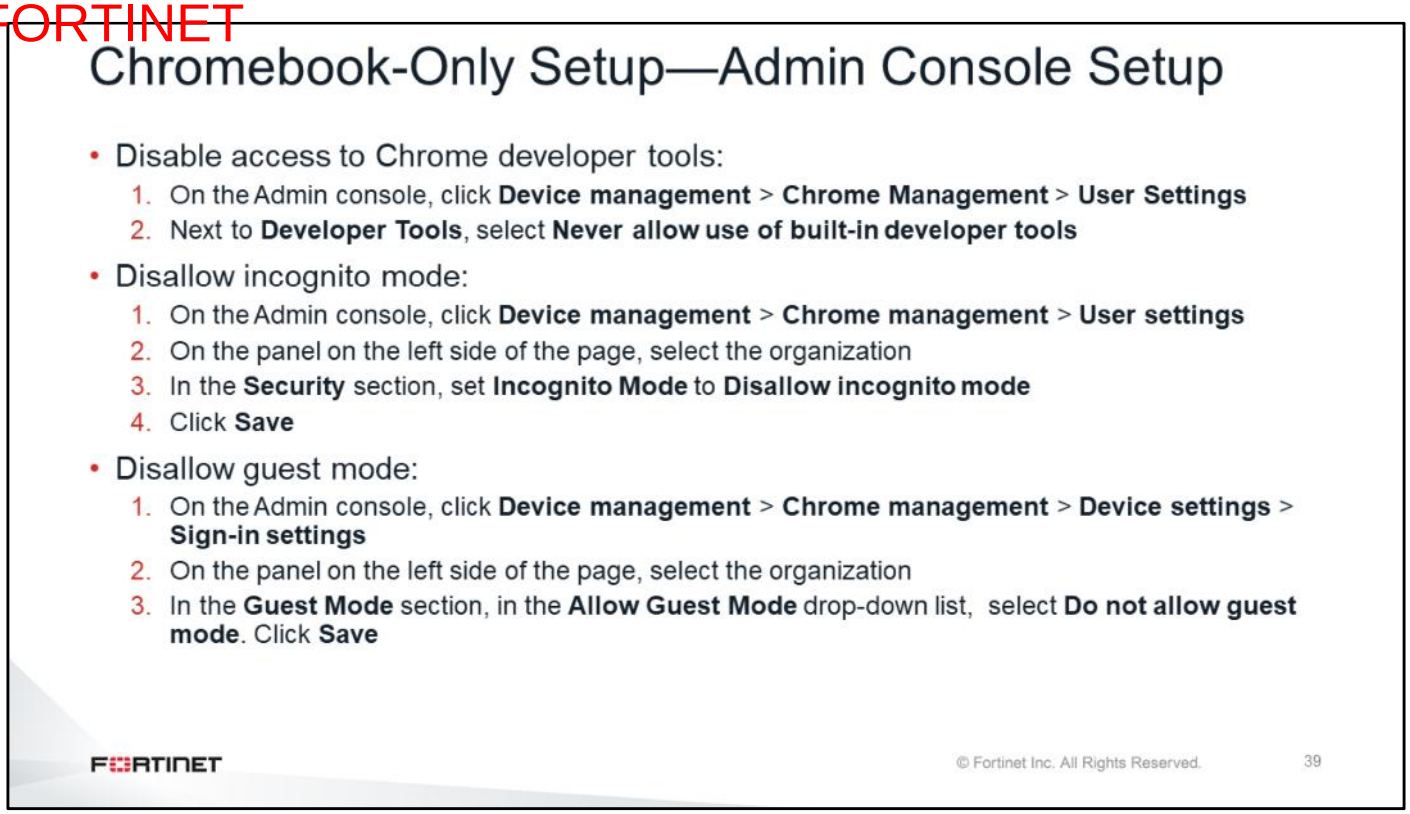
For details about configuration setup, see the *FortiClientEMS Administration Guide*.



The FortiClient Chromebook Web Filter extension communicates with FortiClient EMS using HTTPS connections. You must obtain an SSL certificate and add it to FortiClient EMS to allow the Chromebook extension to trust FortiClient EMS.

If you use a public SSL certificate, you need to add only the public SSL certificate to FortiClient EMS. If you prefer to use a certificate that is not from a common certificate authority (CA), you must add the SSL certificate to FortiClient EMS, and push your certificate's root CA to the Google Chromebooks. Otherwise, the HTTPS connection between the FortiClient Chromebook Web Filter extension and FortiClient EMS will not work.

For more details about certificates, see the *FortiClientEMS Administration Guide*.

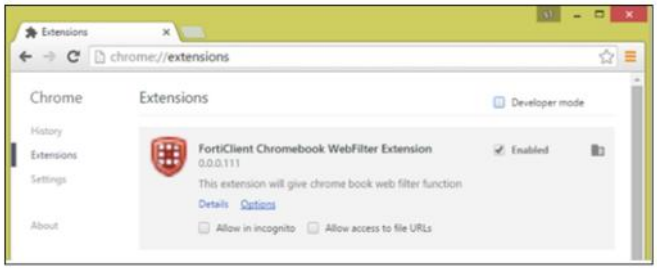


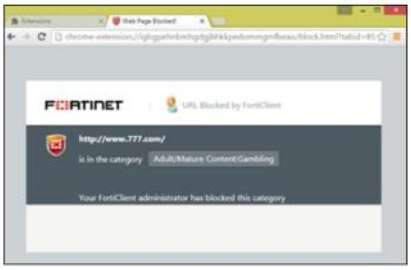
This slide shows the steps required to disable developer tools, incognito, and guest mode. Disabling access to Chrome developer tools blocks users from disabling the FortiClient Web Filter extension.

When users browse in incognito mode, extensions are bypassed.

Chromebook-Only Setup—Admin Console Setup

- Block Task Manager:
  1. On the Google Admin console, click **Device Management** > **Chrome Management** > **User settings** > **Apps and Extensions**
  2. On the panel on the left side of the page, select the organization
  3. In the **Task Manager** drop-down list, select **Block users from ending processes with the Chrome Task Manager**
  4. Verify FortiClient Web Filter

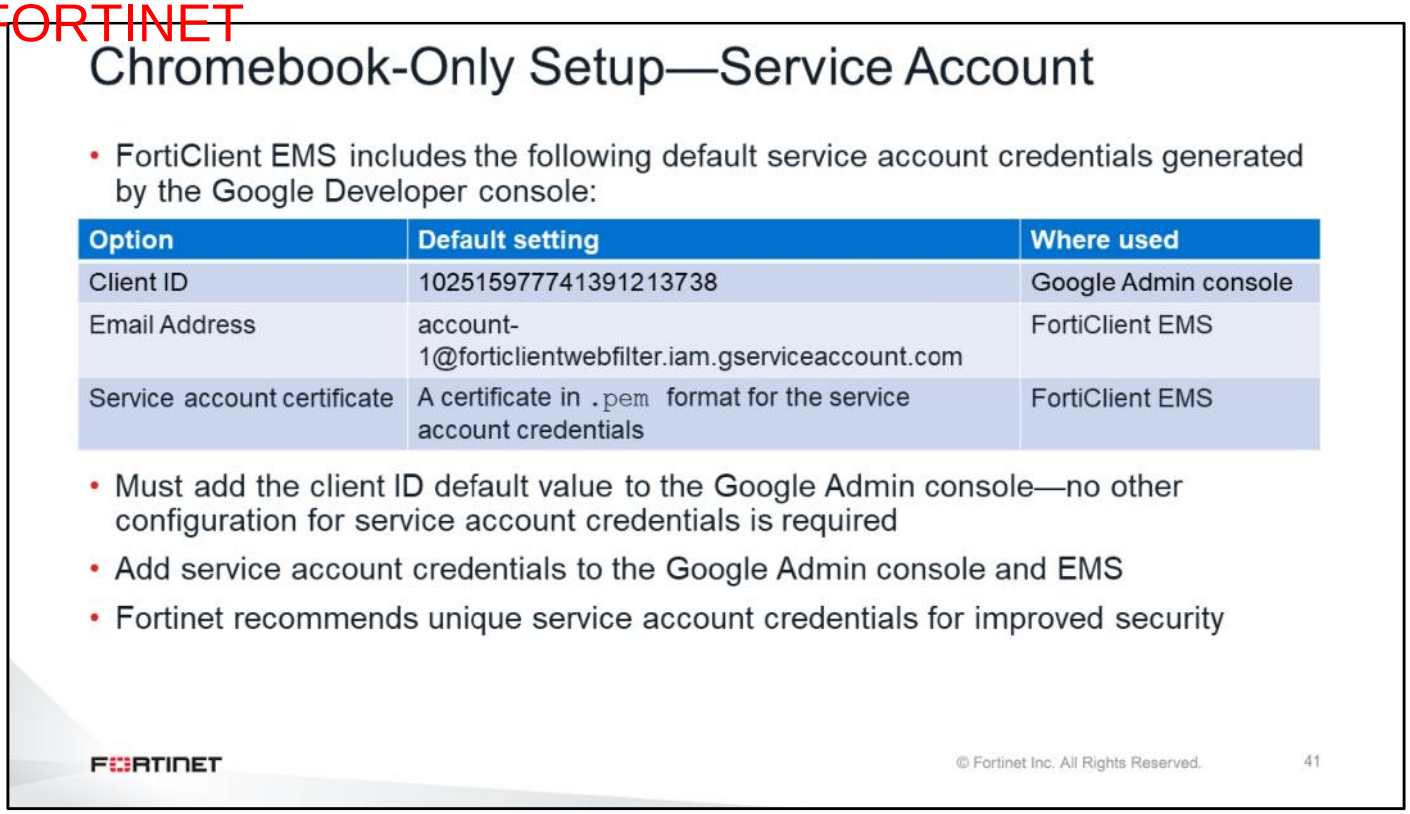




FORTINET © Fortinet Inc. All Rights Reserved. 40

You must block **Task Manager** for managed Google domains as it is shown in this slide. After you add the Google domain to FortiClient EMS, the Google Admin console automatically pushes the FortiClient Web Filter extension to the Chromebooks when users log in to the Google domain.

You can verify that the feature has become available on the Chromebooks by opening the Google Chrome browser. Type `chrome://extensions to check FortiClient extension` and visit any gambling site, such as `http://www.777.com`, and confirm the site is blocked.

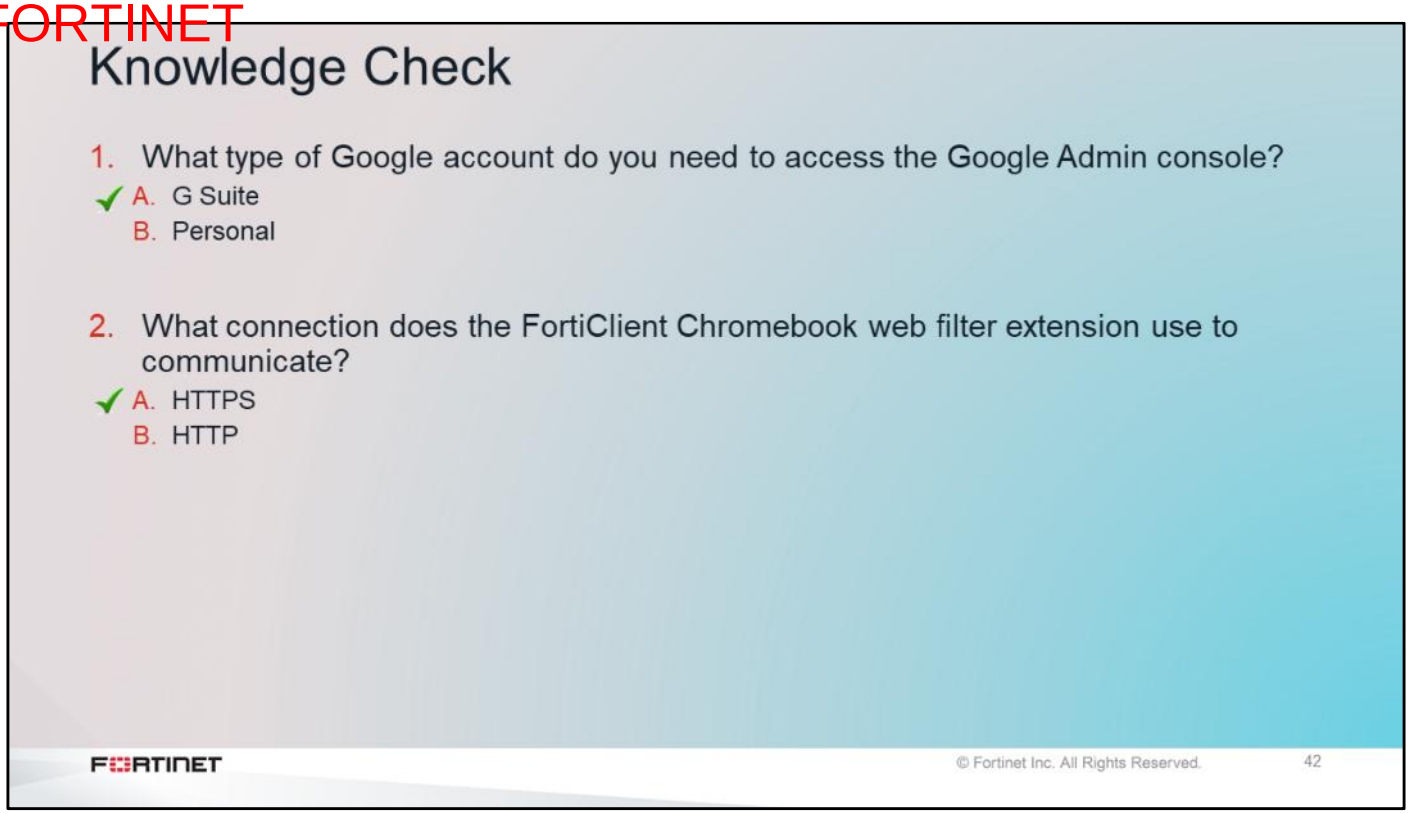


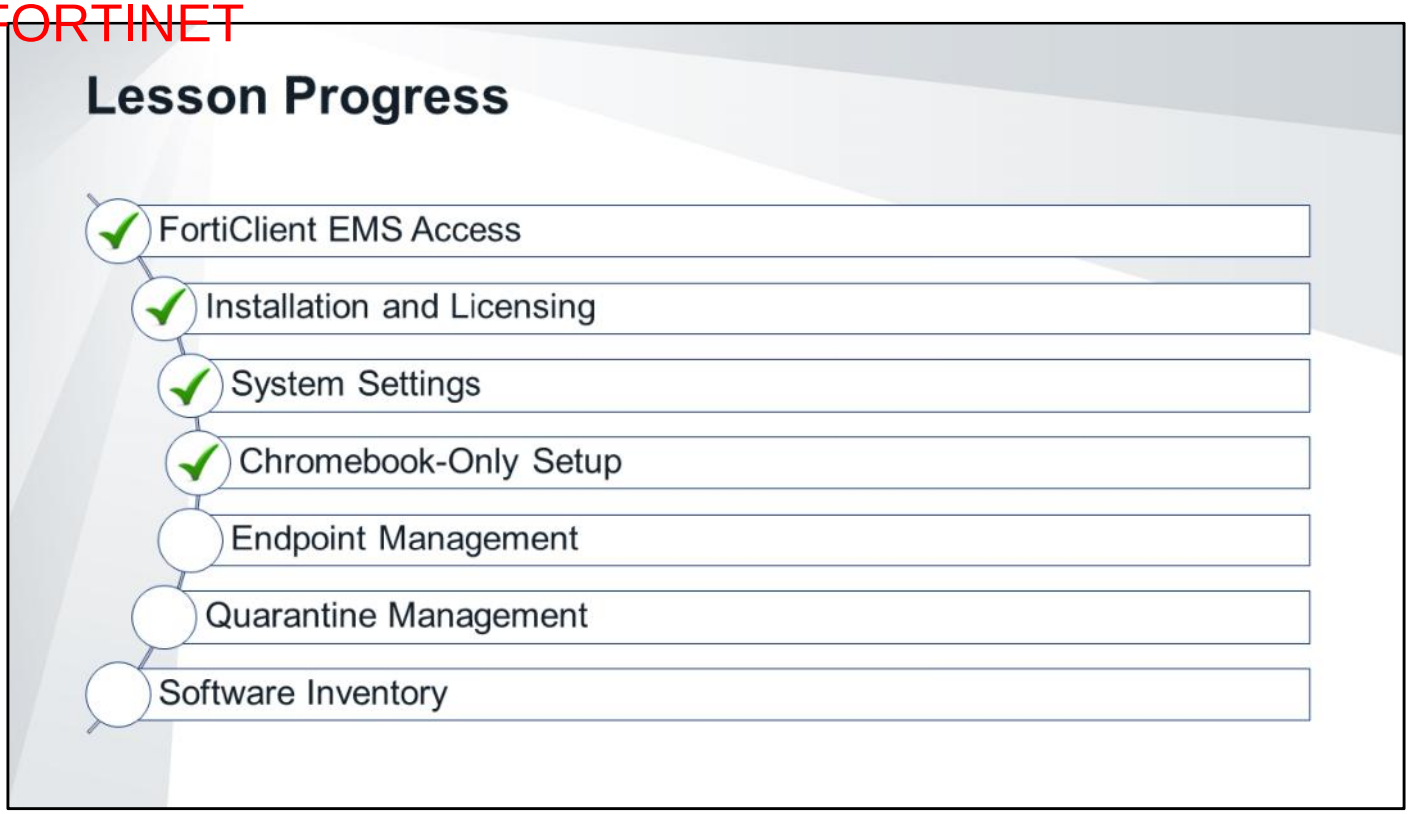
FortiClient EMS requires service account credentials generated by the Google Developer console. You can use the default service account credentials provided with FortiClient EMS. To configure the default service account credentials, you must add the client ID default value to the Google Admin console. No other configuration for service account credentials is required. These settings allow Google to trust FortiClient EMS, which enables FortiClient EMS to retrieve information from the Google domain.

Note that the service account credentials are a set. If you change one credential, you must change the other two credentials.

When using unique service account credentials for improved security, you must complete the following steps to add the unique service account credentials to the Google Admin console and FortiClient EMS:

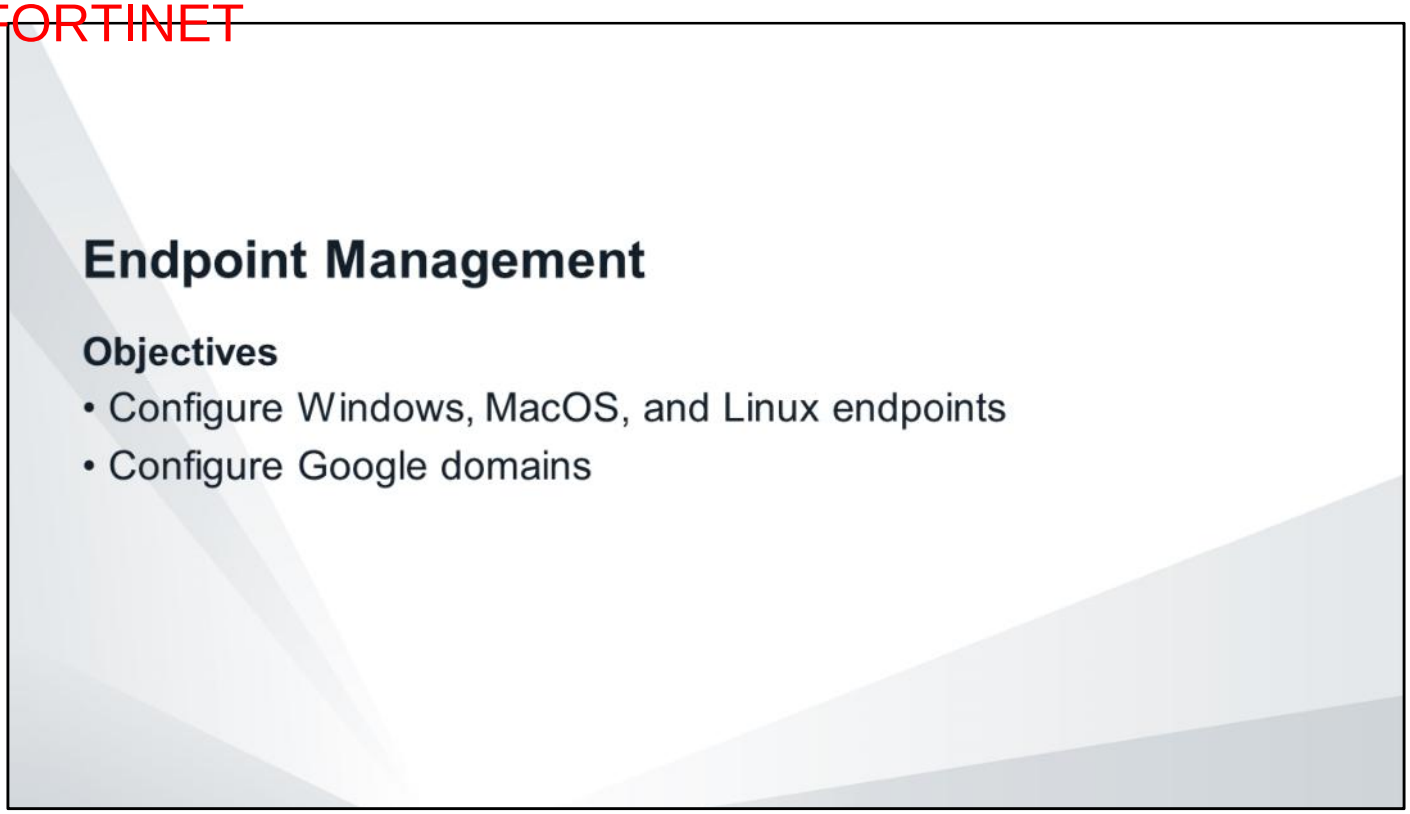
1. Create unique service account credentials using the Google Developer console.
2. Add the unique service account credentials to the Google Admin console.
3. Add the unique service account credentials to FortiClient EMS.





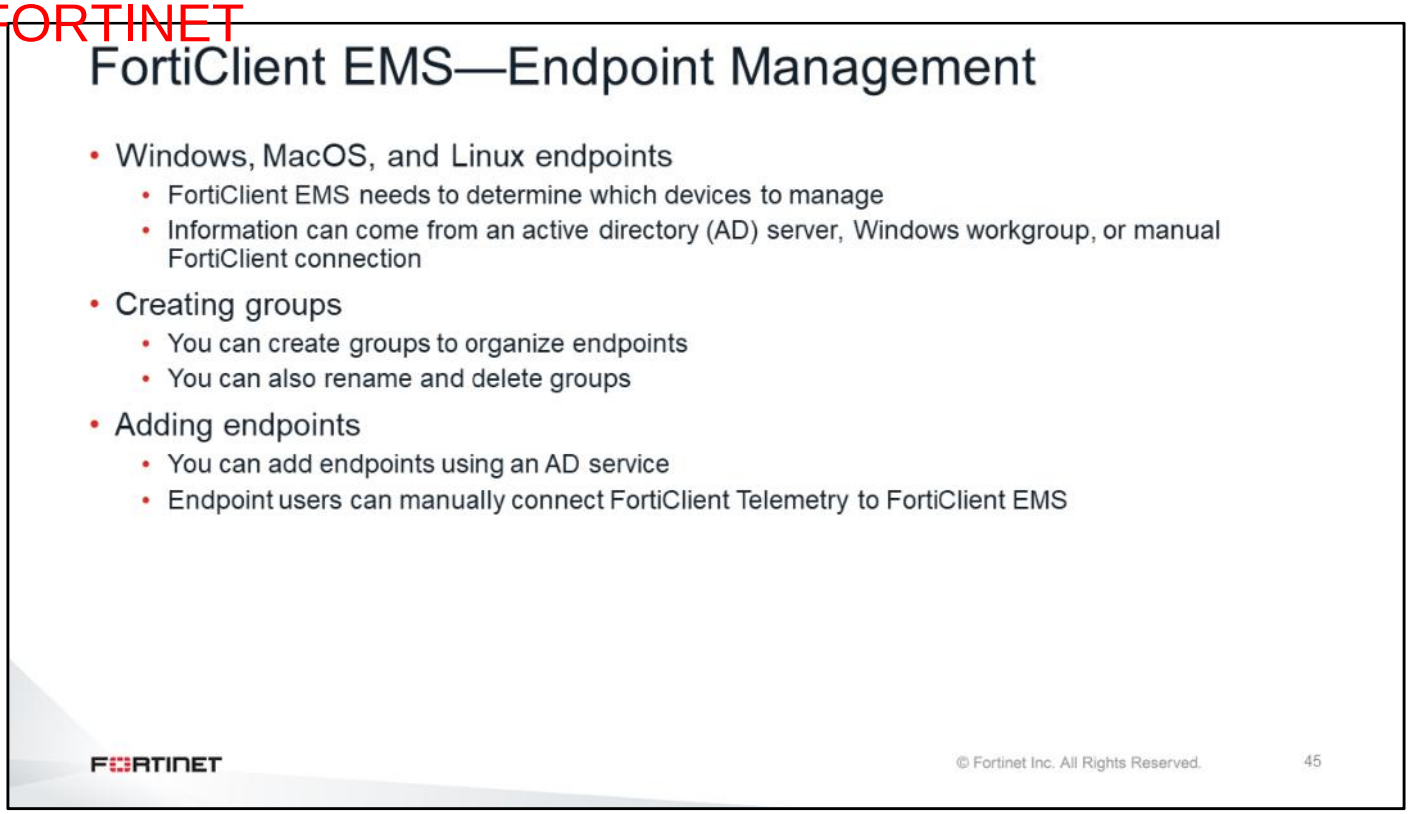
Good job! You now understand how to configure FortiClient EMS to manage Chromebooks.

Now, you will learn about endpoint management.



After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in using FortiClient for endpoint management, you will be able to configure Windows, macOS, and Linux endpoints, as well as Google domains.



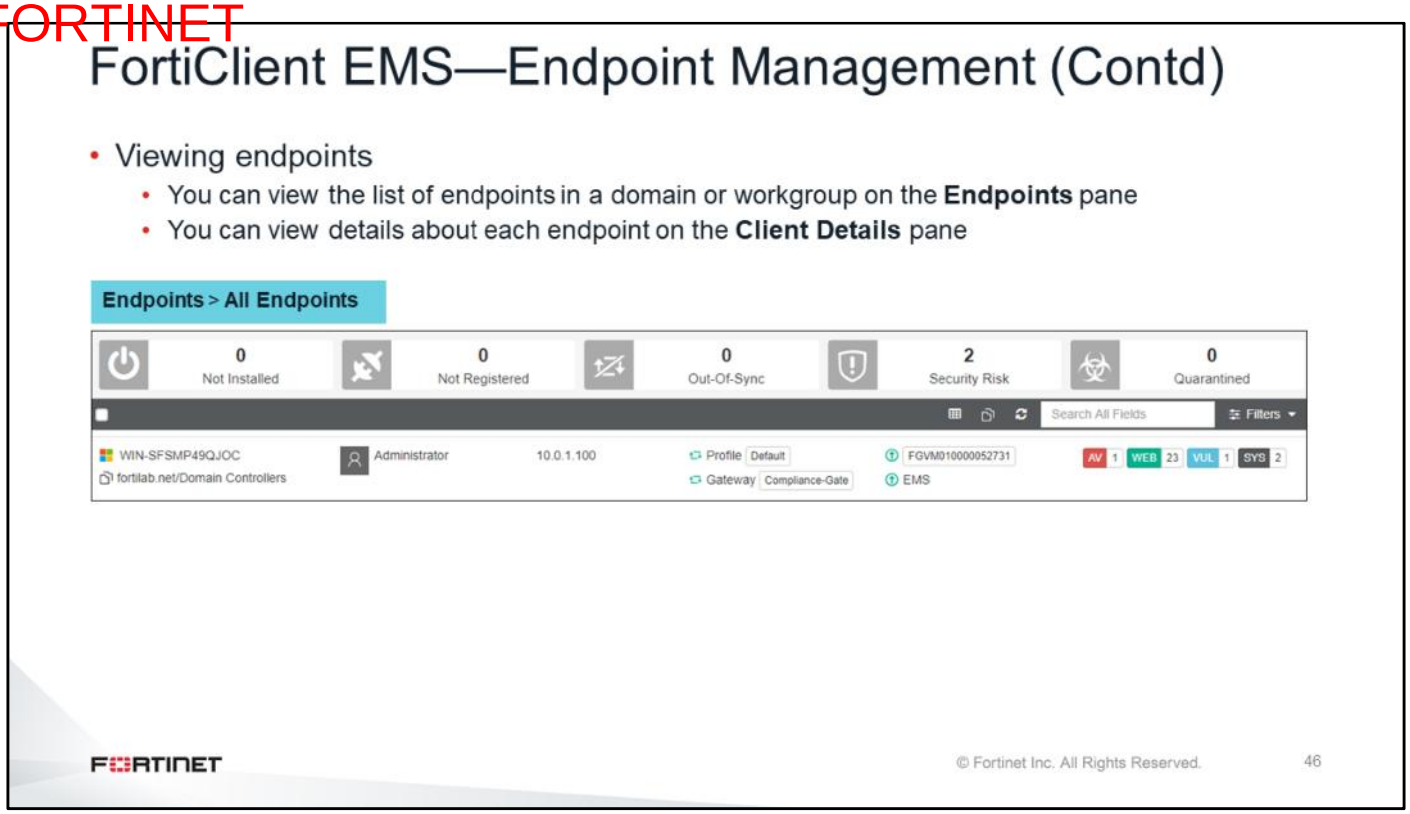
FortiClient EMS needs to identify which devices to manage. For Windows, and macOS, device information can come from an AD server, Windows workgroup, or manual FortiClient connection. The Linux endpoint doesn't communicate with the AD server.

On FortiClient EMS, you can create the domain or workgroup, and then rename and delete groups.

You can import endpoints manually from an AD server. You can import and synchronize information about computer accounts with an LDAP or LDAPS service. You can add endpoints by identifying endpoints that are part of an AD domain server.

Note that after importing endpoints from an AD server, you can edit the endpoints. These changes are not synced back to the AD server.

Endpoint users can also manually connect FortiClient Telemetry to FortiClient EMS by specifying the IP address for FortiClient EMS on FortiClient. This process is sometimes called registering FortiClient to FortiClient EMS.

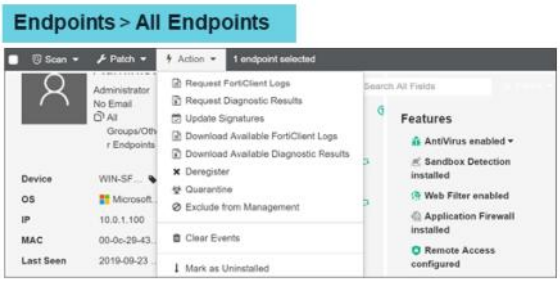


After you add endpoints to FortiClient EMS, you can view the list of endpoints in a domain or workgroup on the **Endpoints** pane. You can also view details about each endpoint on the **Client Details** pane, and use filters to access endpoints with specific qualities.

You can save filter settings as bookmarks, then select the bookmarks to use them.

FortiClient EMS—Endpoint Management (Contd)

- You can manage the following on the **Endpoints** pane:
  - Run antivirus scans on endpoints
  - Run vulnerability scans on endpoints
  - Patch vulnerabilities on endpoints
  - Request FortiClient logs
  - Request the FortiClient diagnostic results
  - Update signatures
  - Unregister and register endpoints
  - Quarantine endpoints
  - Exclude endpoints from management
  - Mark as **Uninstalled**



FORTINET

47

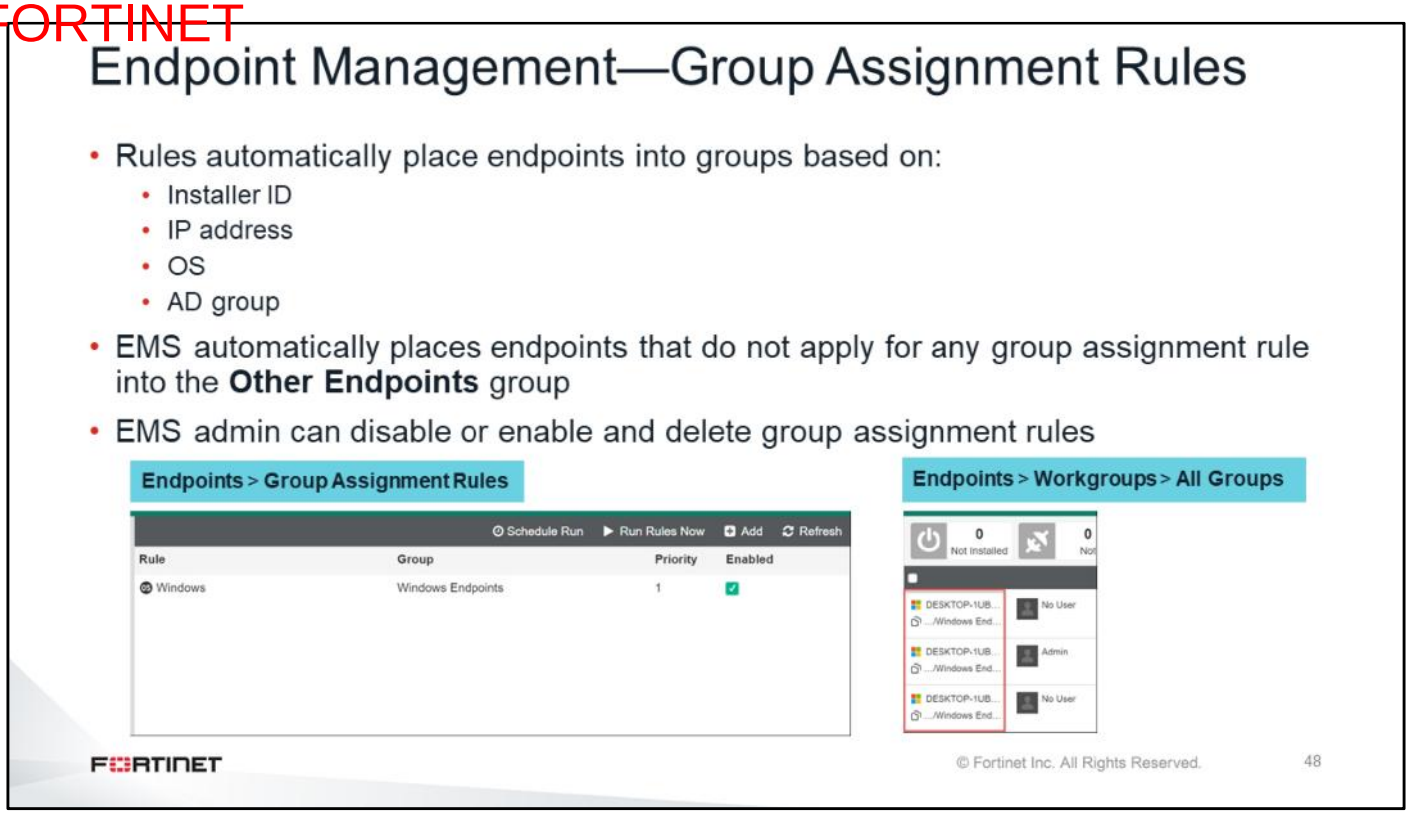
On the **Endpoints** pane, you can perform the actions that are shown in this slide. FortiClient EMS can run antivirus and vulnerability scans. All the scanning starts on the endpoints with the next FortiClient Telemetry communication. You can also view the history of vulnerability scans for each endpoint on the **Client Details** pane.

FortiClient EMS can automatically patch software if a vulnerability requires the endpoint user to download and install a software to patch a vulnerability. The FortiClient console displays the information.

FortiClient can upload a log file from one or several endpoints requested by FortiClient EMS. The log file is uploaded to the hard drive on the computer running FortiClient EMS, and file is not visible in the FortiClient EMS GUI.

You can use FortiClient EMS to run the FortiClient Diagnostic Tool on one or multiple endpoints, and export the results to the hard drive on the computer on which you are running FortiClient EMS. The exported information is not visible in the FortiClient EMS GUI.

FortiClient EMS can also quarantine, disconnect and connect, exclude from management, and delete endpoints.



You can use group assignment rules to automatically place endpoints into custom groups based on their installer ID, IP address, OS, or AD group.
Creating a FortiClient 6.2+ deployment package includes an option to specify an installer ID. For example, say you want all endpoints located in your company's headquarters to be moved in the same endpoint group. You can configure a FortiClient 6.2.1 deployment package with an "HQ" installer ID, then deploy this deployment package to the desired endpoints.

IP Address option allows you to create a group assignment rule that automatically moves all endpoints within a specified subnet or IP address range into the same custom group.

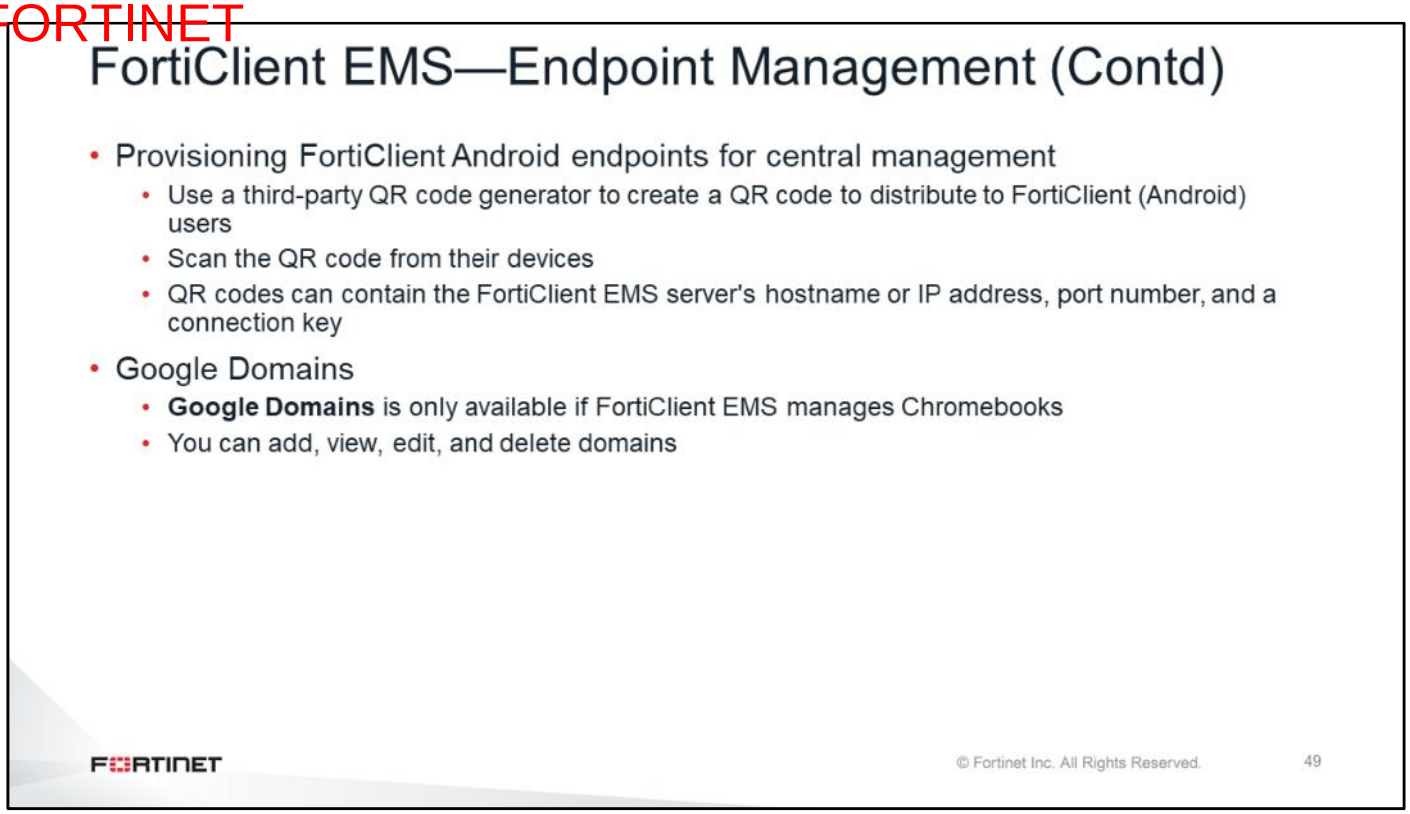
OS option automatically moves all endpoints that have a specific OS installed into the custom group.

AD Group option creates a group assignment rule to automatically move all endpoints in a selected AD group into the custom group.

When the endpoints' FortiClient connects to FortiClient EMS, FortiClient EMS places them in the desired group.

If a newly connected endpoint does not match any group assignment rule and belongs to an imported AD domain, the endpoint is moved into the OU to which it belongs in the AD domain tree. If no AD domain has been imported, or the endpoint also does not belong to the imported AD domain, it is placed in the **Other Endpoints** group.

FortiClient EMS automatically places endpoints that do not apply to any group assignment rule into the **Other Endpoints** group.

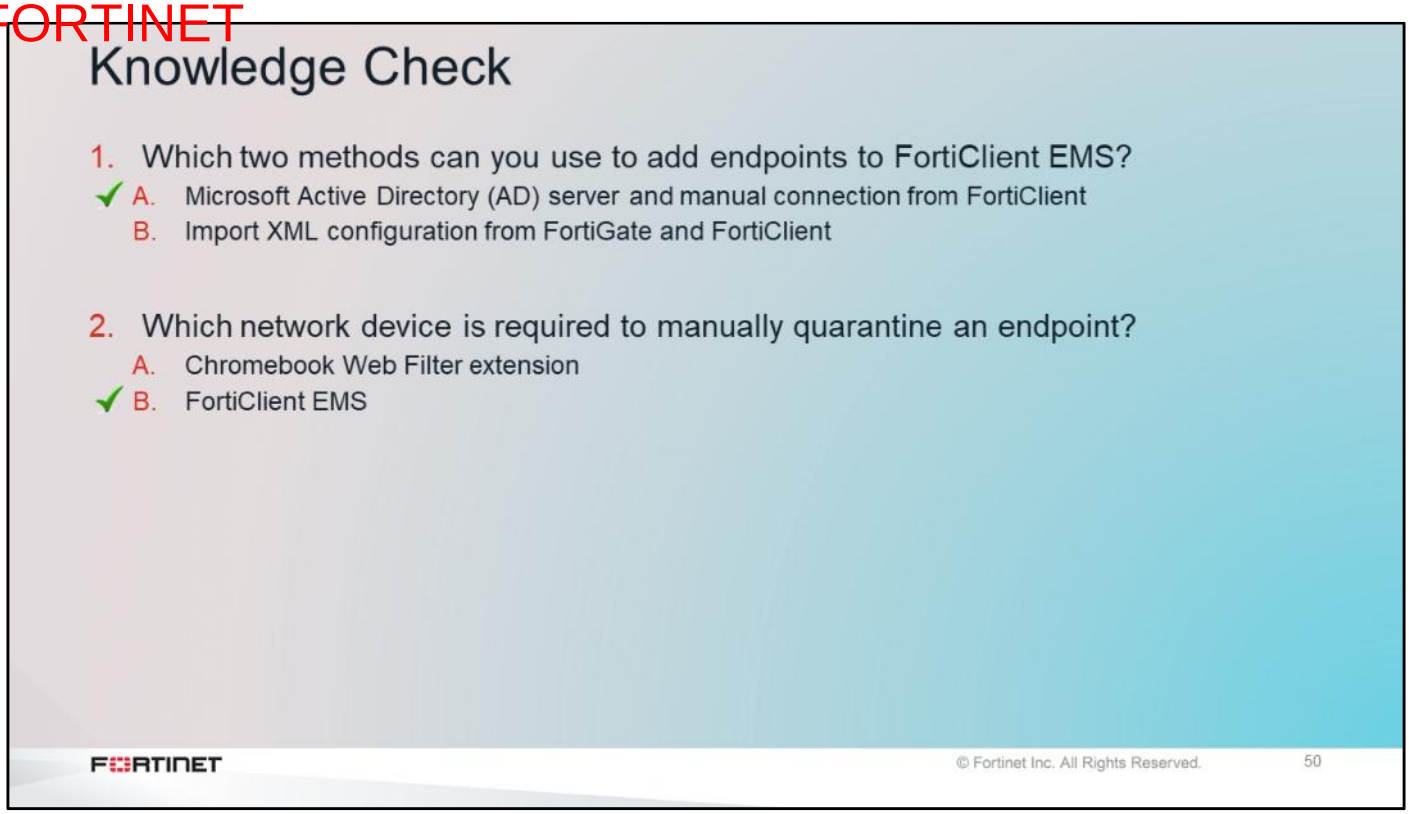


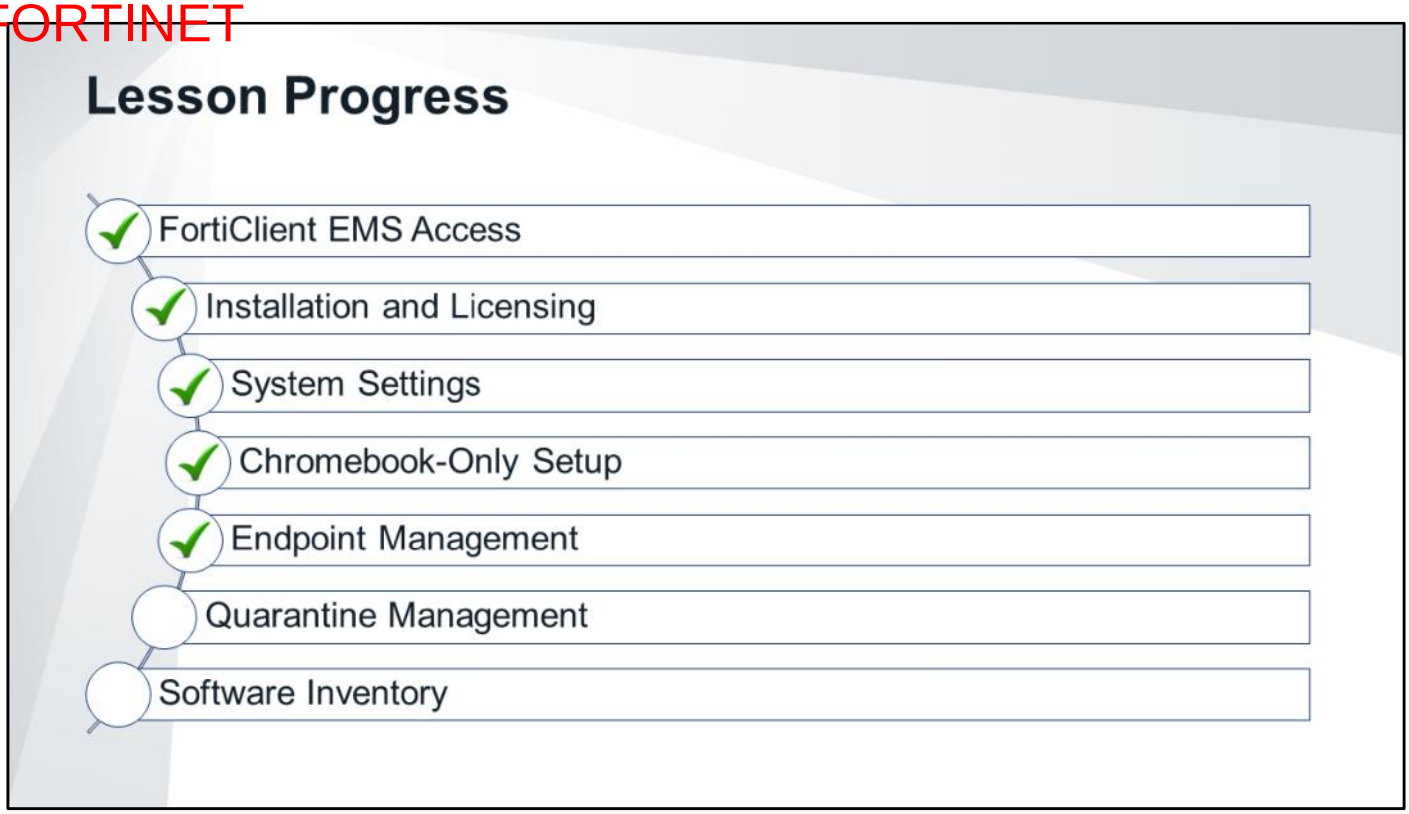
You can use a third-party QR code generator to create a QR code to distribute to FortiClient (Android) users. FortiClient (Android) users can scan the QR code from their devices to automatically enable FortiTelemetry and attempt a connection to the specified FortiClient EMS server and FortiGate device. QR codes can contain the FortiClient EMS server hostname or IP address, port number, and a connection key. Only the FortiClient EMS hostname/IP address is required; all other fields are optional.

FortiClient EMS needs to identify which devices to manage. Device information comes from the Google Admin console. **Google Domains** option is available if **EMS for Chromebooks Settings** is selected in EMS server settings.

You can add domains on the **Manage Domains** page on the FortiClientEMS. After you add domains to FortiClient EMS, you can view, edit, and delete them.

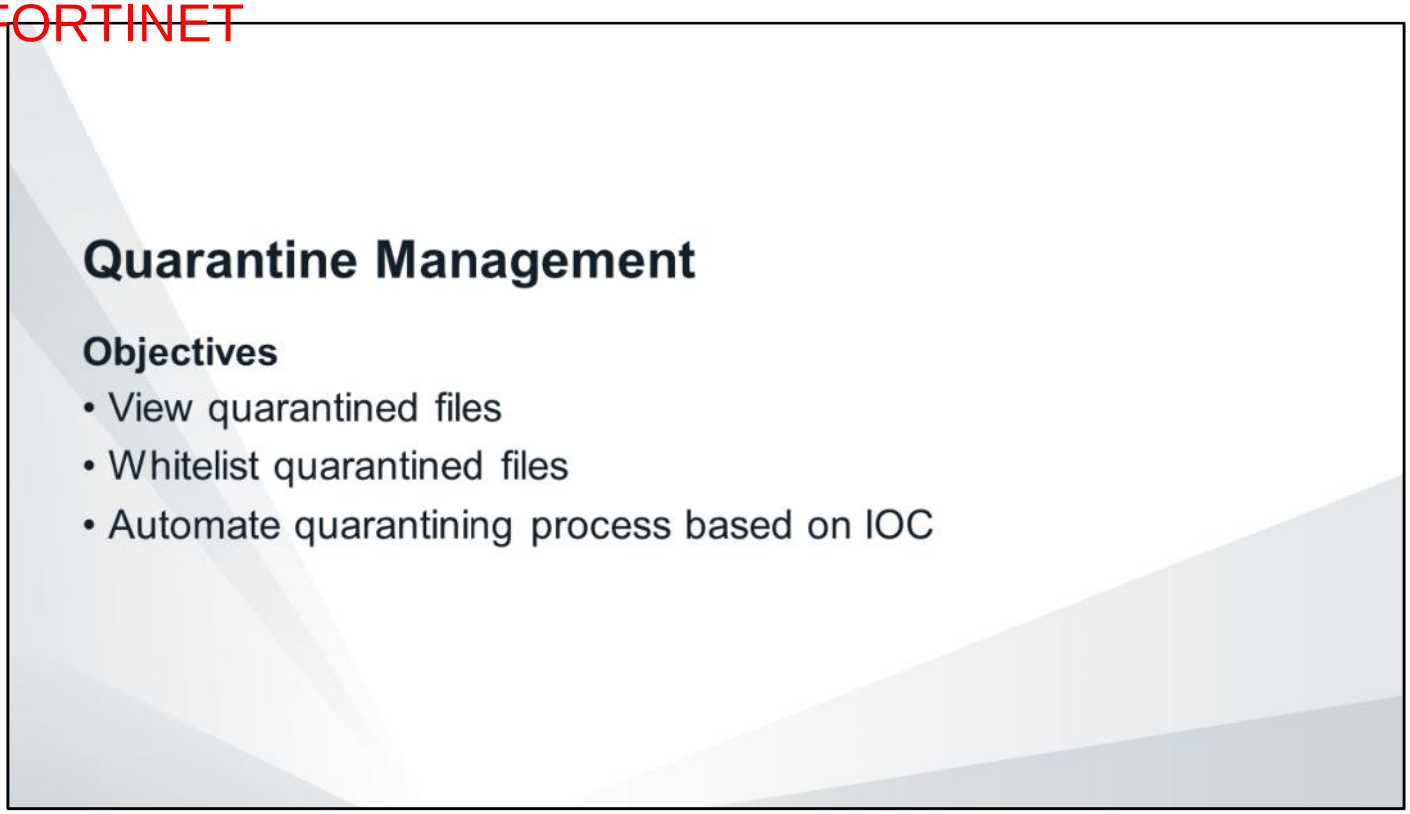
Note that this section is applicable only if you are using FortiClient EMS to manage Google Chromebooks.





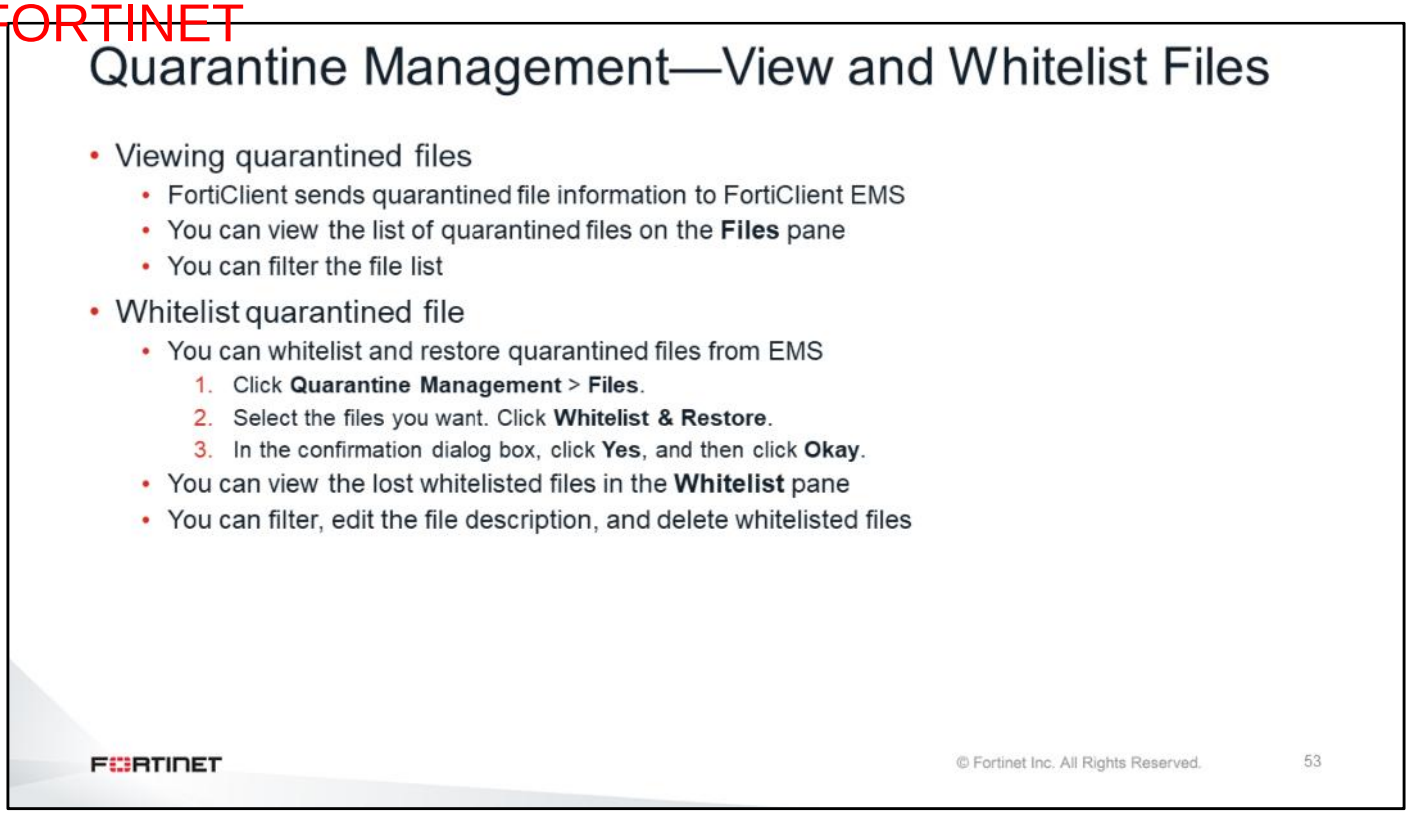
Good job! You now understand endpoint management for Windows, macOS, Linux, and Chromebook user endpoints on FortiClient EMS.

Now, you will learn about quarantine management.



After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in using FortiClient EMS to manage quarantined files, you will be able to view and whitelist quarantined files.

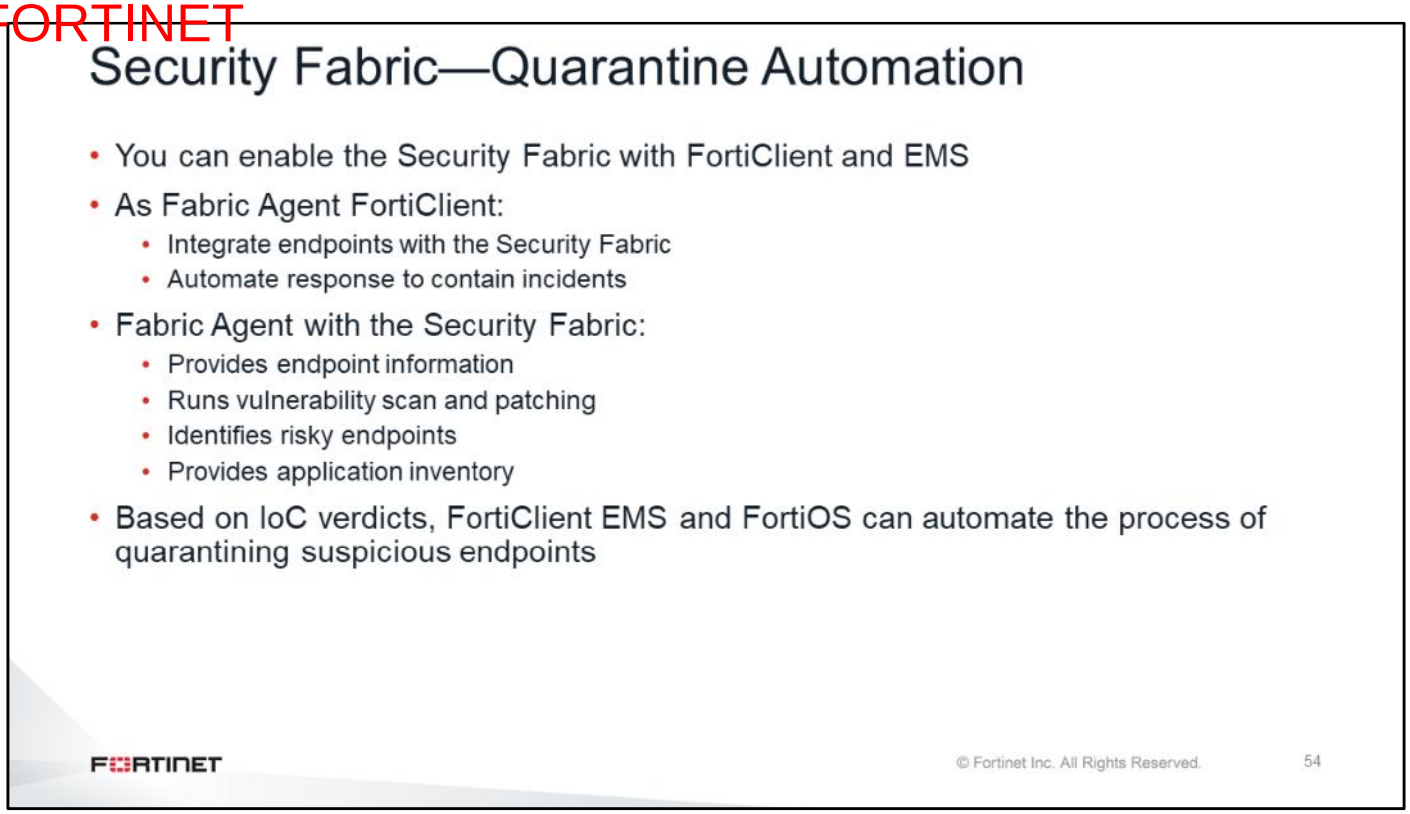


On the **Files** pane, the FortiClient EMS administrator can view quarantined file information for all managed endpoints, and whitelist files from FortiClient EMS, if needed.

FortiClient sends quarantined file information to FortiClient EMS. After FortiClient quarantines files on endpoints and sends the quarantined file information to FortiClient EMS, you can view the list of quarantined files on **Quarantine Management** on **Files** pane. You can also view details about each quarantined file and use filters to access quarantined files that have specific qualities.

You can whitelist and restore quarantined files from EMS. The steps are shown in this slide. This releases the files from quarantine and makes them accessible on the endpoint with the next telemetry communication between FortiClient EMS and FortiClient. The file status changes to **Quarantined & Whitelisted**.

Note that the FortiClient console doesn't allow you to restore and delete quarantined files. These options are grayed out on the FortiClient GUI.



Many of you have heard of the Security Fabric. The Security Fabric uses FortiTelemetry to link different security sensors and tools together to collect, coordinate, and respond to malicious behaviour anywhere it occurs on your network, in real-time.

The Fabric Agent connects endpoints with the Security Fabric, and delivers endpoint visibility and control by sharing endpoint telemetry and compliance status with the Security Fabric. It also has vulnerability management capabilities to extend the scanning process to either the managed FortiGate or EMS.

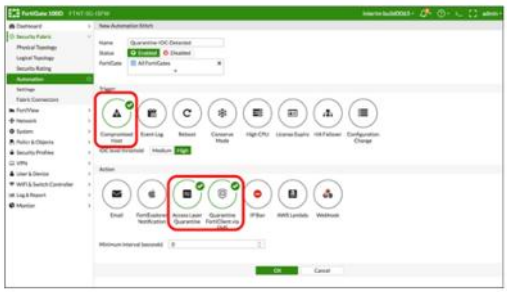
In the Security Fabric topology, you can see the compromised and quarantined endpoints. You can obtain the visibility and details about these endpoints from devices such as FortiAnalyzer, where indicator of compromise (IoC) verdicts are based on a threshold value that is reached or exceeded, at which point an endpoint becomes a risk, must be quarantined, and is confirmed to be compromised.

In addition to quarantining malicious files, submitting objects to FortiSandbox for analysis, and applying patches, by integrating with the Security Fabric, FortiClient can also automate the process of quarantining suspicious or compromised endpoints.

The benefits of quarantine automation include, containing threats and incidents, and controlling outbreaks.

Quarantine Automation (Contd)

- You can quarantine an endpoint from FortiOS using EMS using an API
- The following network components are required:
  - FortiGate
  - FortiAnalyzer
  - FortiClient EMS
  - FortiClient
- Security Fabric, which includes the above network devices, can automatically quarantine an endpoint on which an IoC is detected



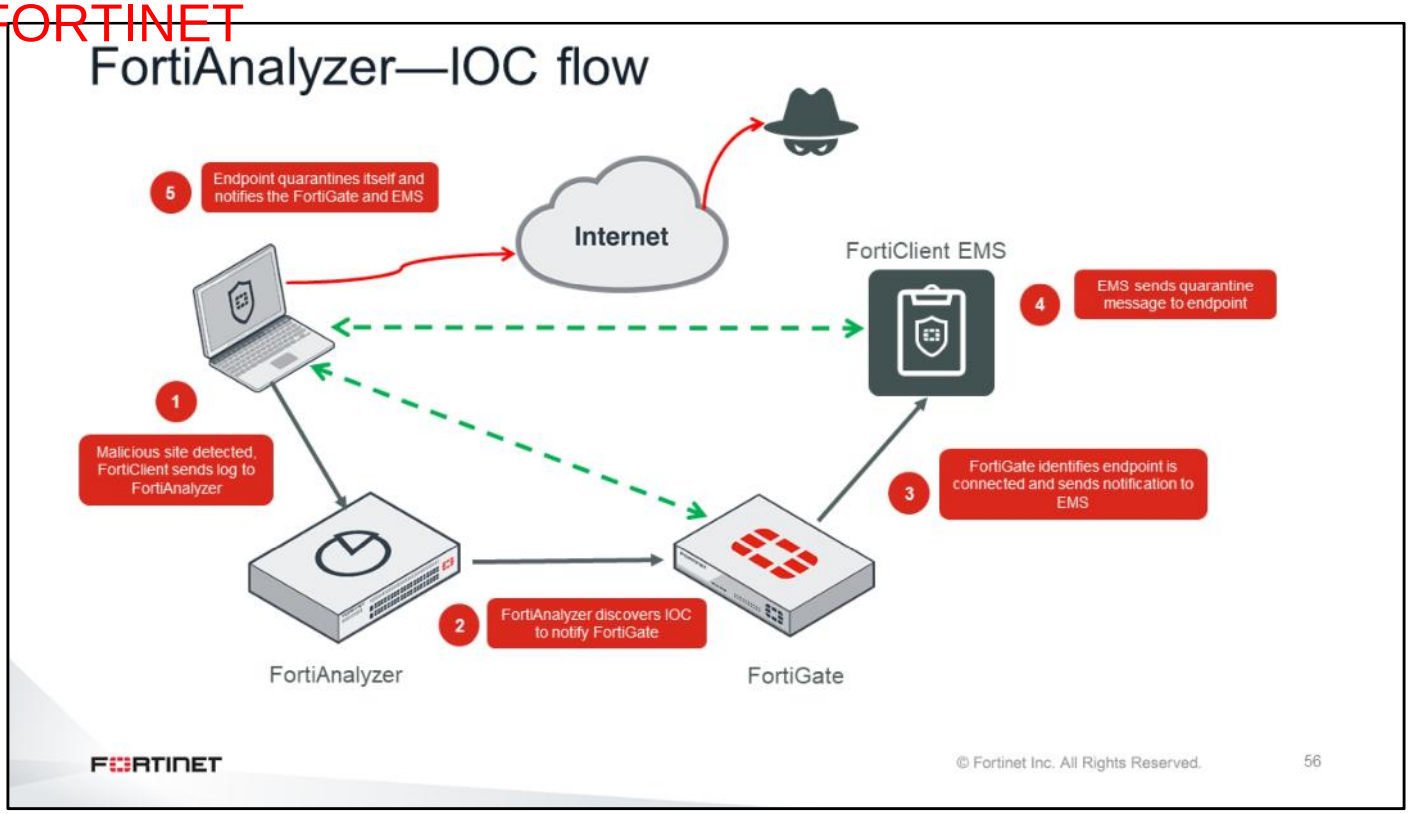
FORTINET

55

The Security Fabric offers visibility of endpoints at various monitoring levels. When the Security Fabric includes network devices listed here, you can configure the system to automatically quarantine an endpoint on which an IOC is detected. This requires the following network devices:

- FortiGate
- FortiAnalyzer
- FortiClient EMS
- FortiClient

You must connect FortiClient to both the EMS and FortiGate. FortiGate and FortiClient must both be sending logs to FortiAnalyzer. You must configure the EMS IP address on the FortiGate, as well as administrator login credentials.



This configuration functions as follows:

1. FortiClient sends logs to FortiAnalyzer.
2. FortiAnalyzer discovers IoCs in the logs and notifies FortiGate.
3. FortiGate identifies if FortiClient is a connected endpoint, and if it has the login credentials for the EMS that FortiClient is connected to. With this information, FortiGate sends a notification to EMS to quarantine the endpoint.
4. EMS searches for the endpoint and sends a quarantine message to it.
5. The endpoint receives the quarantine message and quarantines itself, blocking all network traffic. The endpoint notifies FortiGate and EMS of the status change.

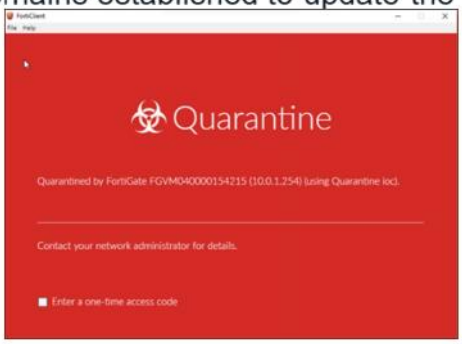
Executing automation:
The following command triggers the quarantine action on the endpoint at `endpoint_ip_address`:

- `diag endpoint forticlient-ems-rest-api queue-quarantine-ipv4 endpoint_ip_address`

Note that this feature is not supported on FortiClient (Linux).

Endpoint Management—Quarantine Automation

- FortiClient must connect to both the EMS and FortiGate
- FortiGate must have an EMS IP address and credentials to log in
- FortiAnalyzer must receive logs from both FortiGate and FortiClient
- Quarantine is done at the network interface driver level (IPS)
- Communication with EMS remains open to unquarantined endpoint
- Telemetry to FortiGate remains established to update the status



FORTINET

57

You must meet the following prerequisites for FortiClient, EMS, and FortiGate:

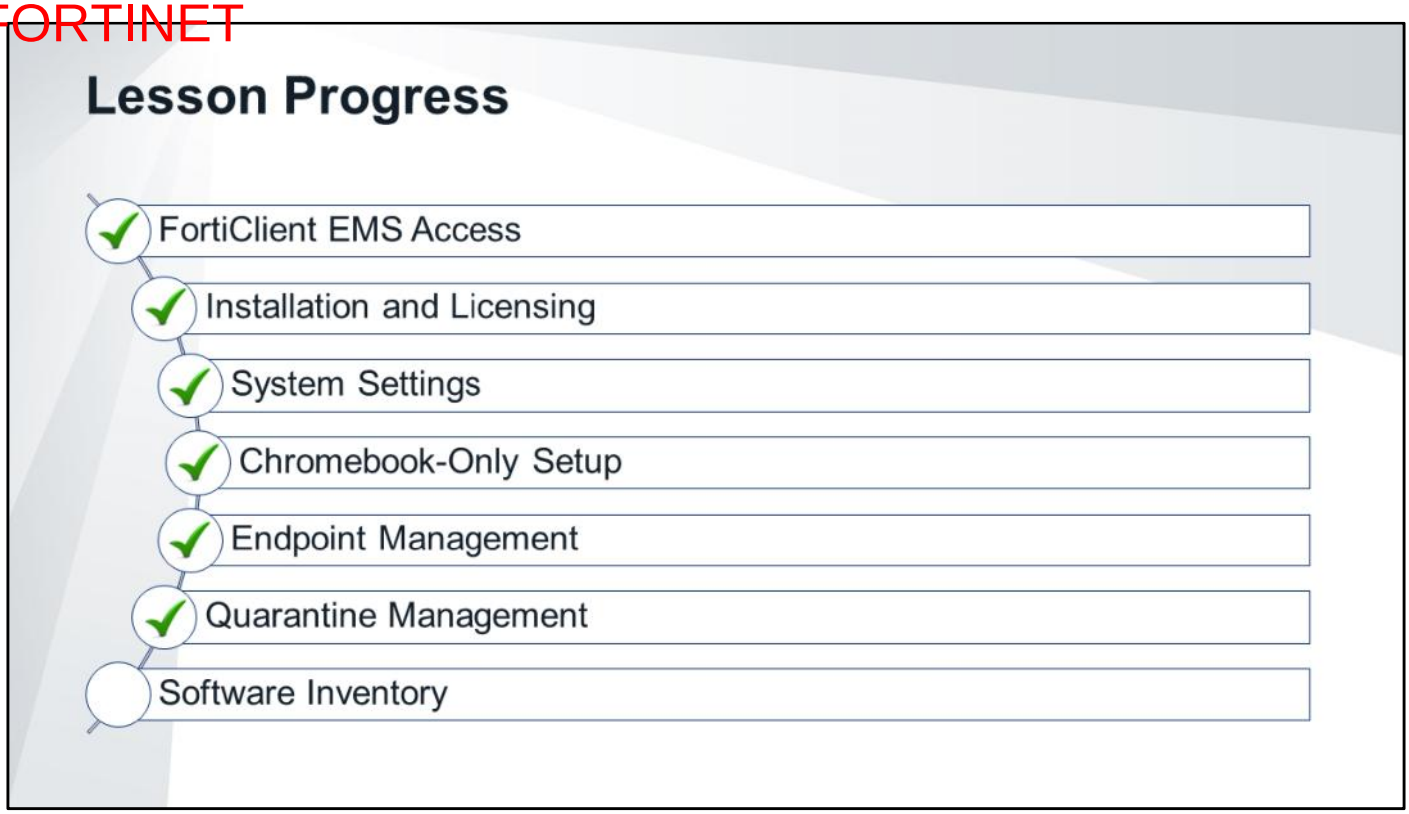
1. FortiClient must be installed on the endpoint and connected to both EMS and FortiGate.

2. On EMS, an endpoint profile and gateway list using the FortiGate IP address, must be assigned to the endpoint. It also needs an endpoint policy that is configured with the desired profile and telemetry gateway list for the desired endpoint group, and the **Remote HTTPS access** option must be enabled.

3. FortiGate must use the following configuration to quarantine an endpoint.

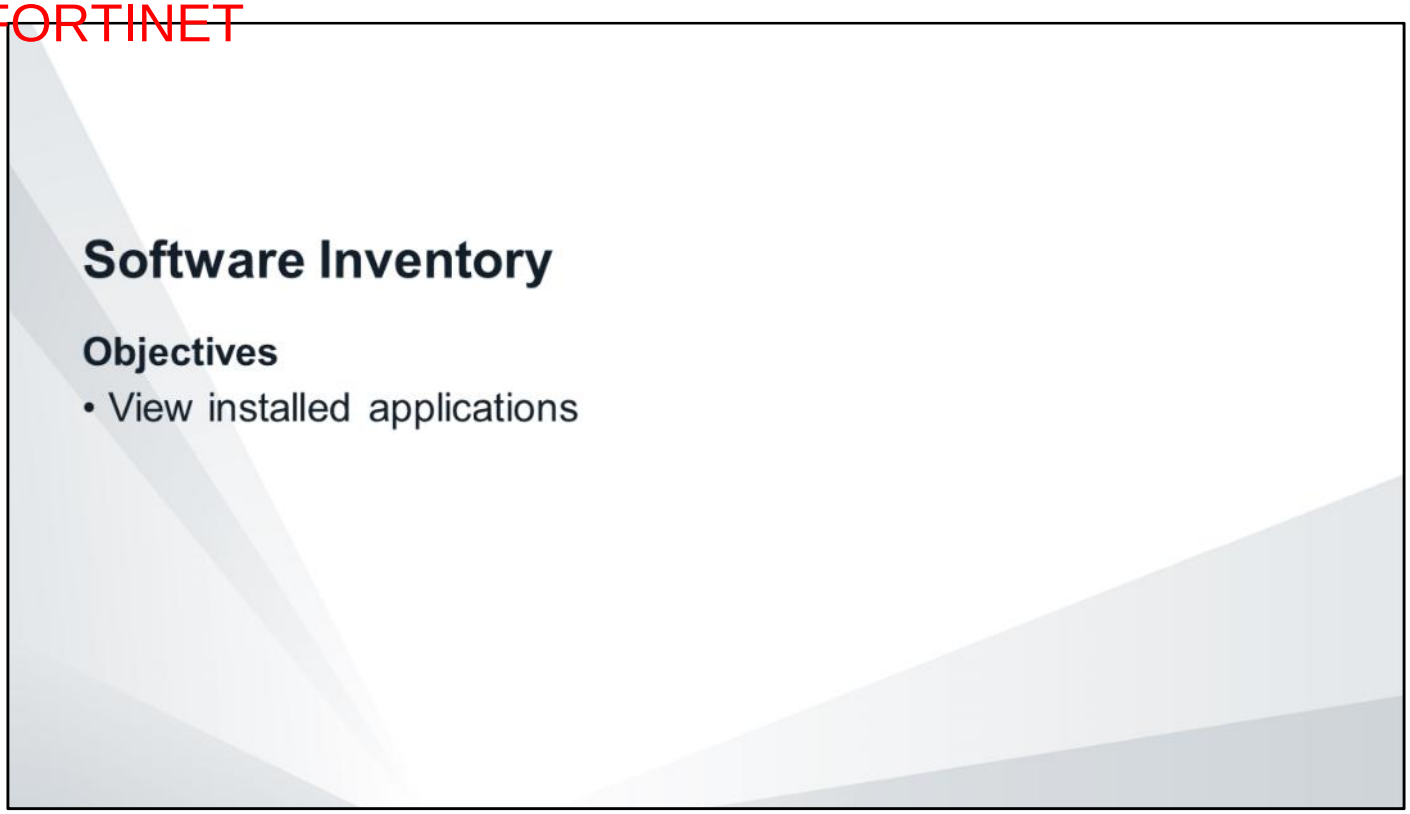
- Automation trigger
- Automation action
- Automation stitch
- EMS firewall address object
- Endpoint control FCT-EMS object

For more details about FortiGate automation configuration, see the *FortiClientEMS 6.2 Administration Guide*.



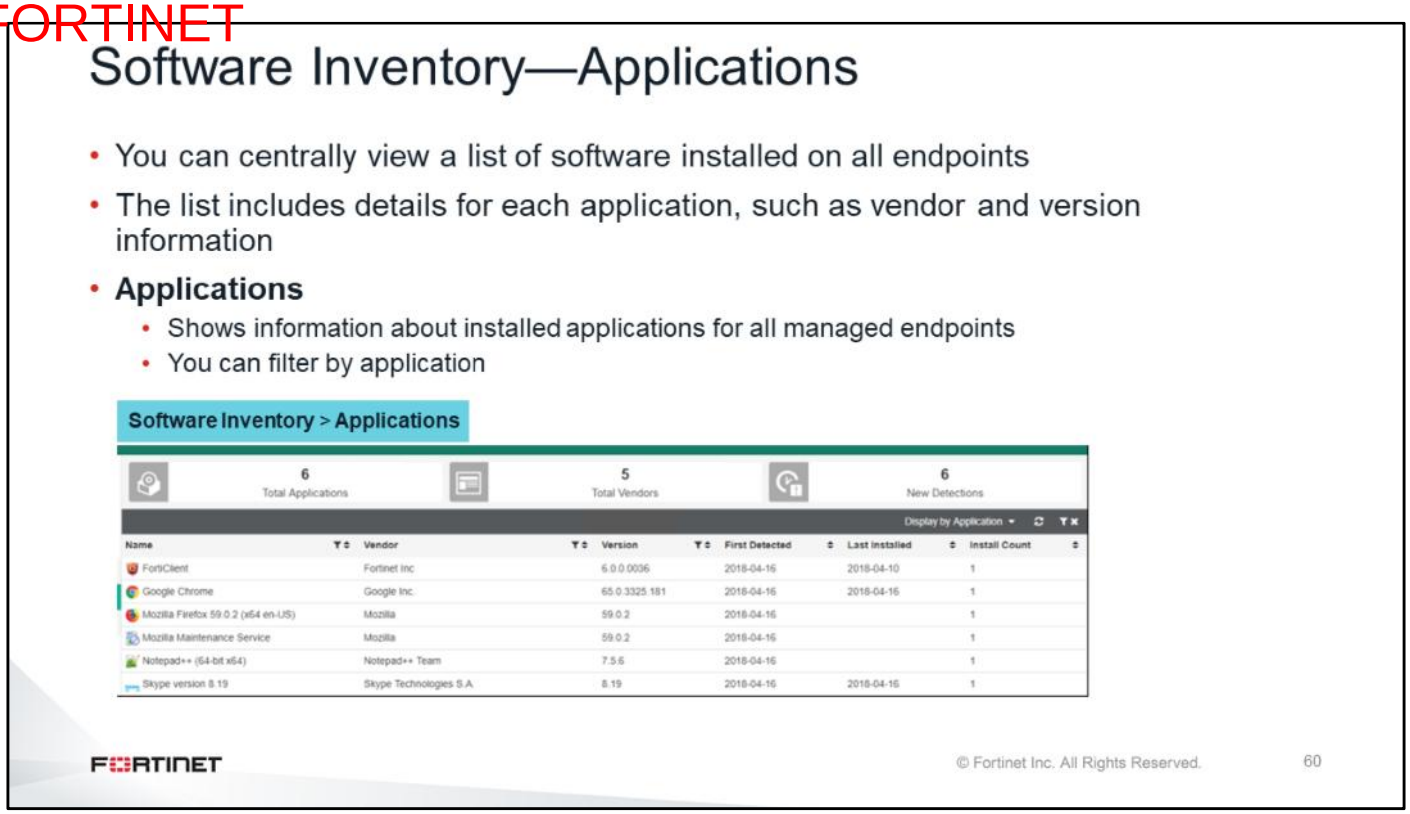
Good job! You now know how to configure FortiClient XML.

Now, you will learn about FortiClient EMS.



After completing this section, you should be able to achieve the objectives shown on this slide.

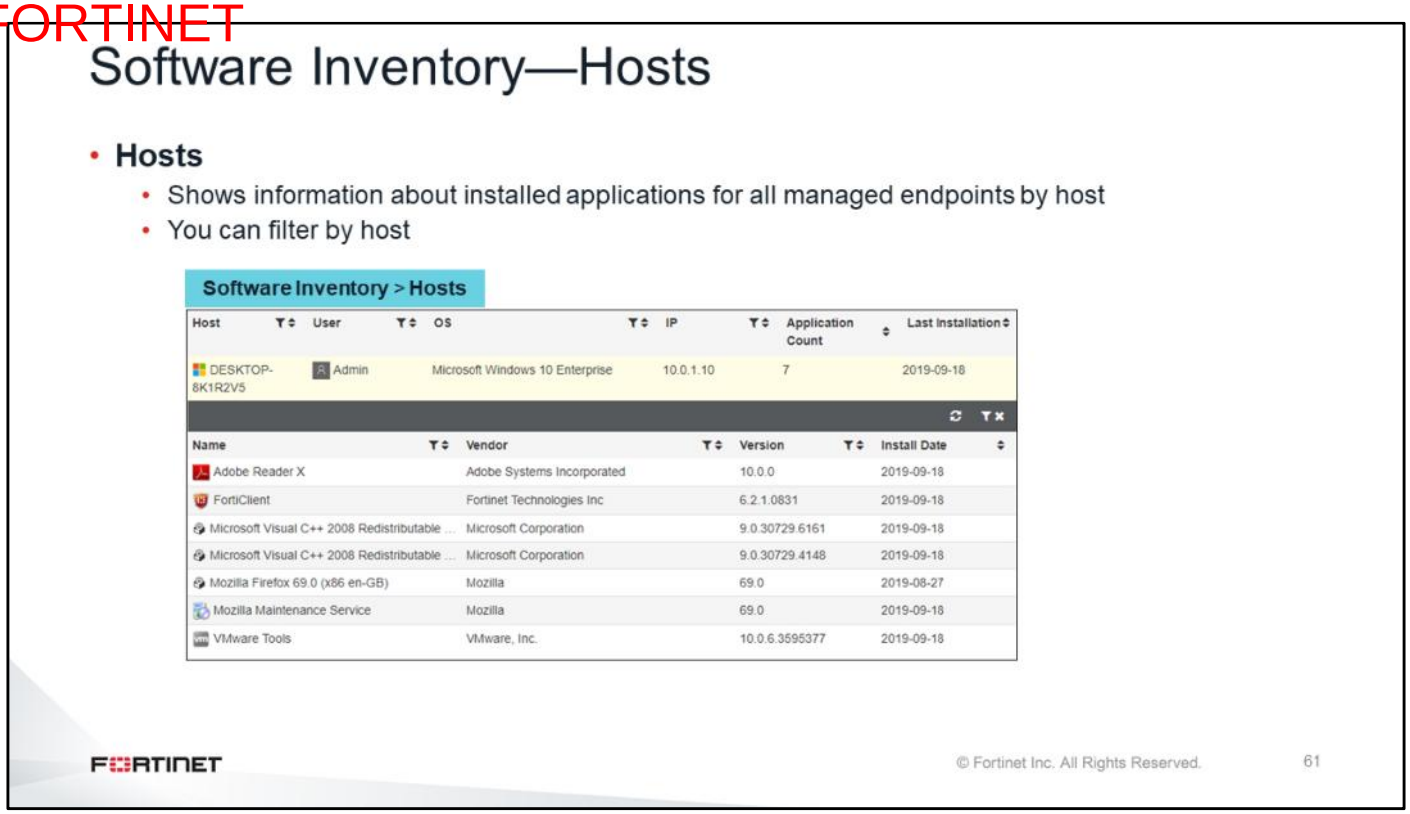
By demonstrating competence in using FortiClient EMS to view the software inventory on endpoints, you will be able to identify what applications are installed.



You can centrally view a list of software installed on all endpoints. The list includes details for each application, such as vendor and version information. You can view this information by application or by vendor, on the **Applications** pane, or by host on the **Hosts** pane. FortiClient sends installed application information to FortiClient EMS.

The FortiClient EMS administrator can view installed application information for all managed endpoints on the **Applications** pane.

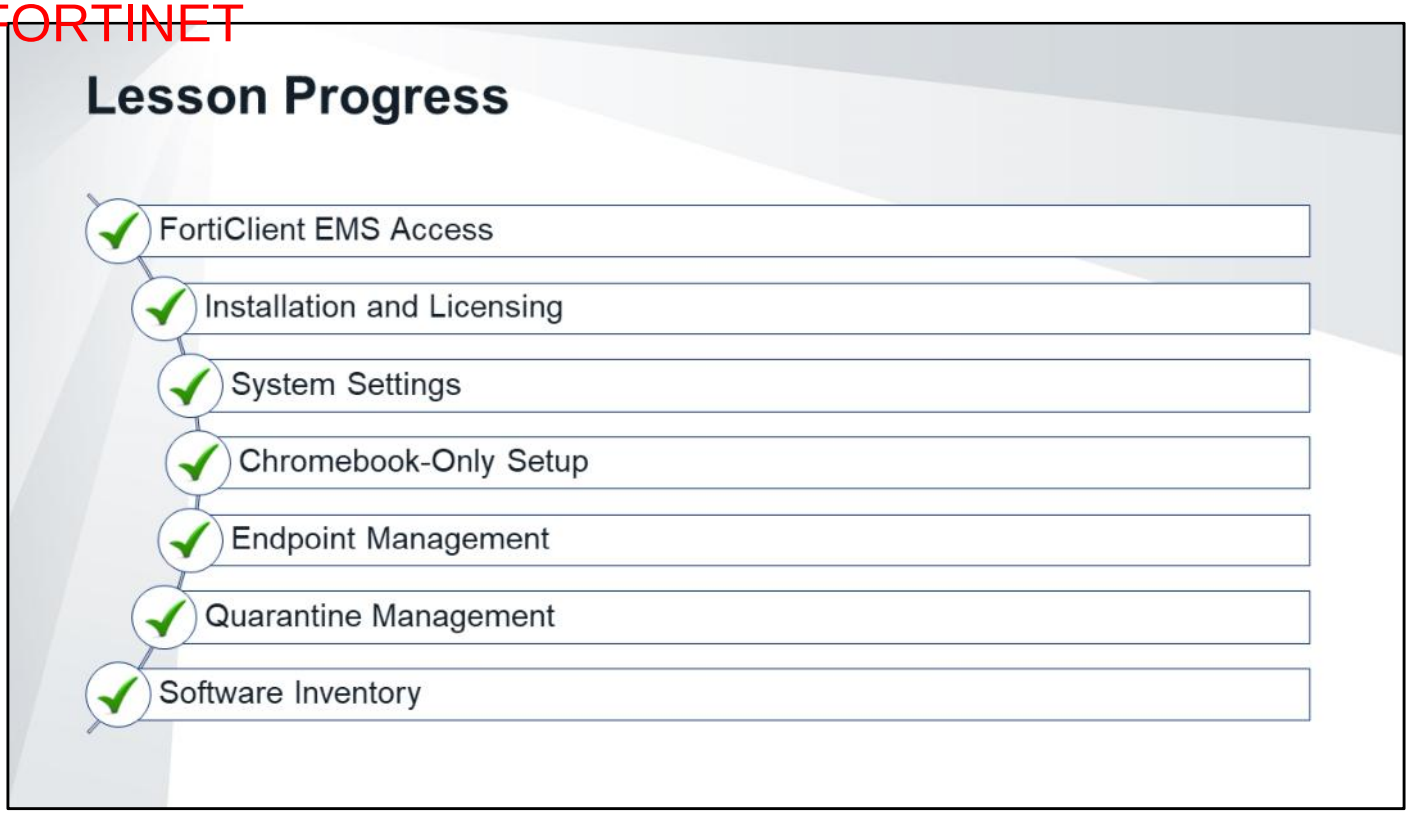
The **Applications** pane also shows the total number of application installed, vendors, and newly installed applications. You can view the application names alphabetically, or by vendor. You can also apply filters by application name, vendor name, and version number.



The FortiClient EMS administrator can view installed applications information for all managed endpoints by host on the **Hosts** pane.

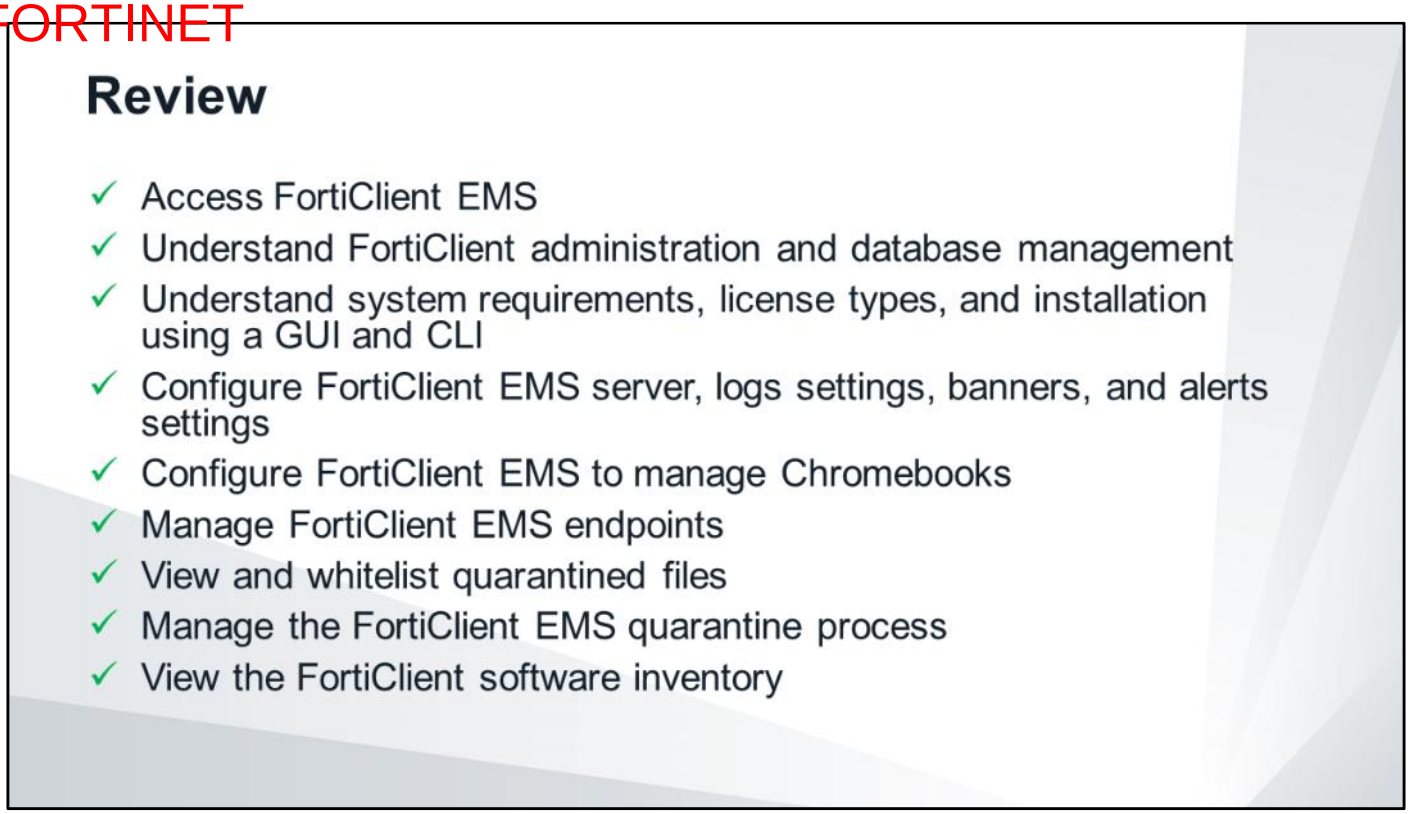
The **Hosts** pane shows the total number of applications, OS details, and lists of the software installed on the endpoints. You can also view other details about the hosts, as shown on this slide image.

You can apply filters by host name, user name, OS name, and IP address.



Congratulations! You have completed this lesson.

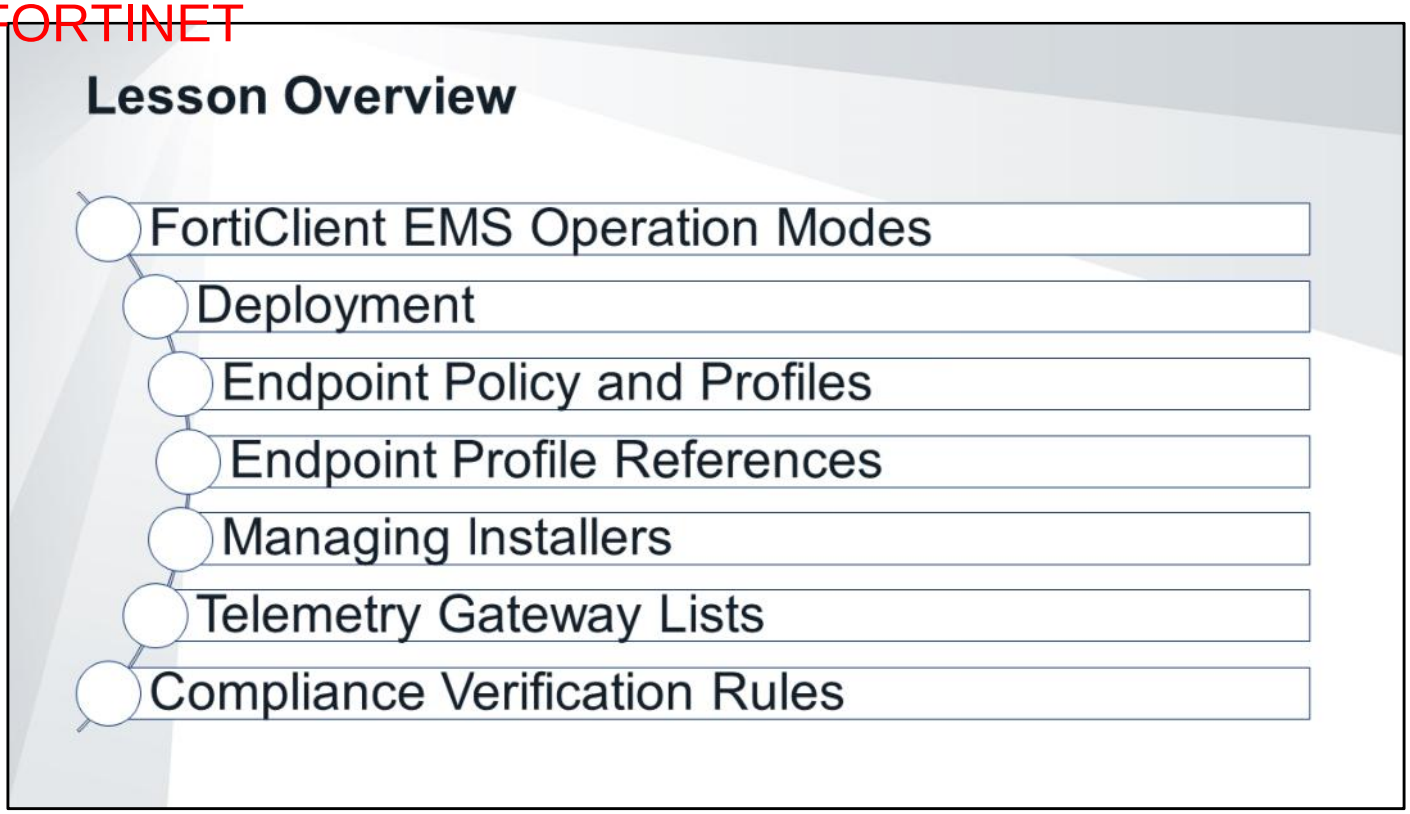
Now, you will review the objectives that you covered in this lesson.



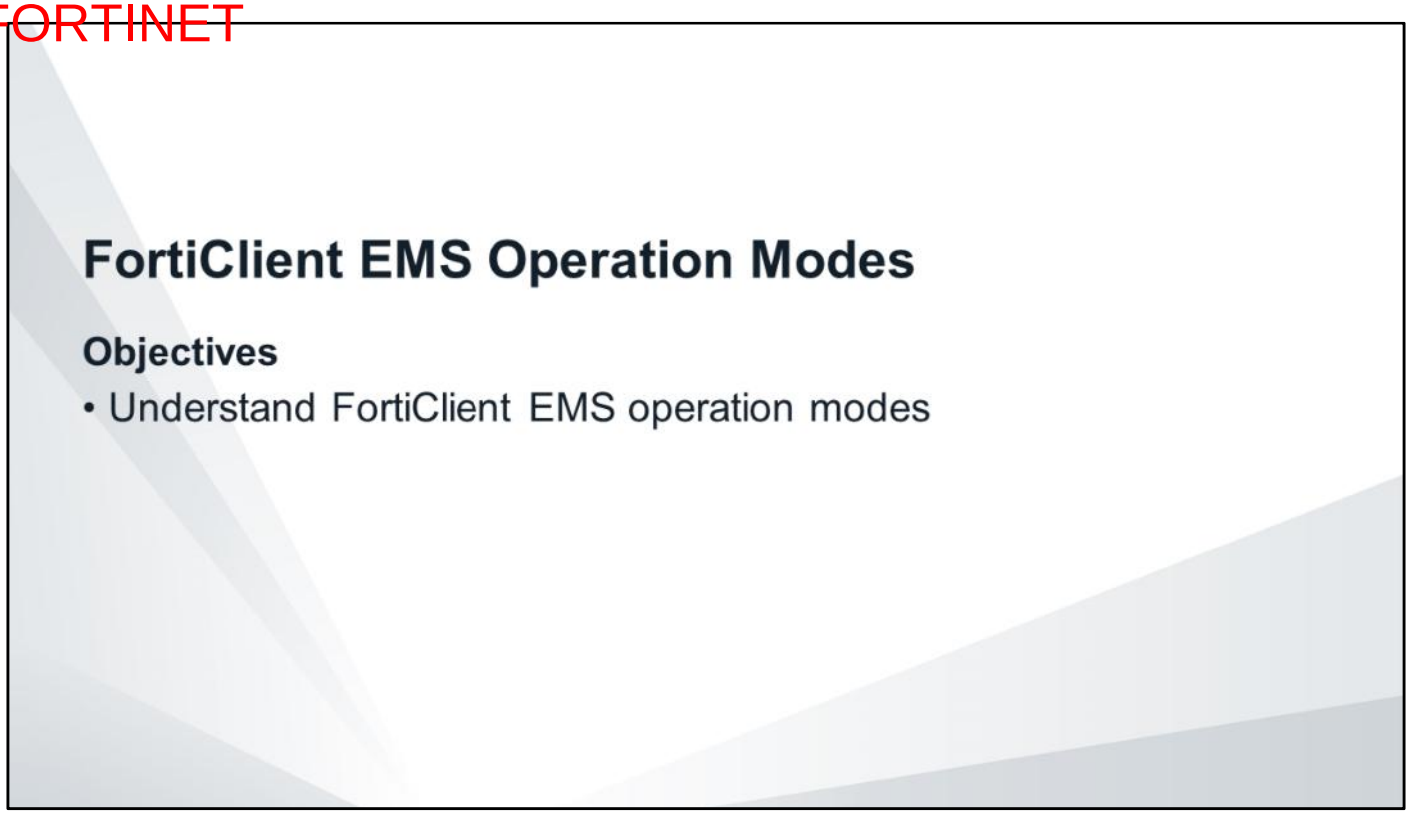
This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to install, configure, and administer FortiClient EMS. You also learned how to manage a large number of endpoints.

In this lesson, you will learn how to deploy, provision, and manage FortiClient on endpoints using FortiClient EMS.



In this lesson, you will learn about the topics shown on this slide.

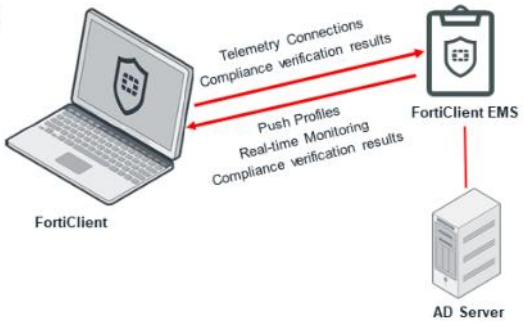


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence understanding FortiClient EMS, you will be able to use it effectively in your network.

Standalone Mode Without Security Fabric

- FortiClient EMS provides FortiClient endpoint provisioning
- FortiClient endpoints connect FortiClient Telemetry to FortiClient EMS to receive configuration information from FortiClient EMS
- EMS sends compliance verification rules to FortiClient
- EMS controls the connection between FortiClient and EMS
- FortiClient settings are locked
- Endpoint status shows as **Managed by EMS**



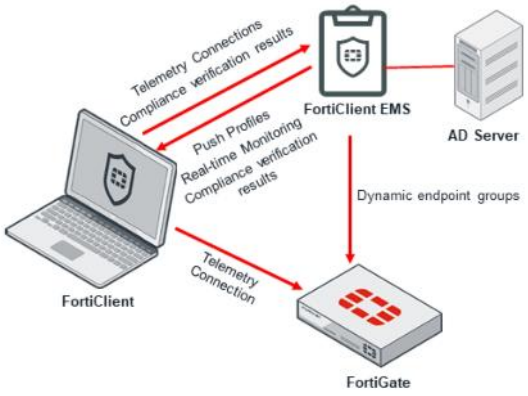
FORTINET

4

FortiClient EMS in standalone mode provides FortiClient endpoint provisioning. FortiClient endpoints connect FortiClient Telemetry to FortiClient EMS to receive configuration information inn an endpoint profile as part of an endpoint policy from EMS. EMS also sends compliance verification rules to FortiClient, and uses the results from FortiClient to dynamically group endpoints in EMS. Only EMS can control the connection between FortiClient and EMS. Any changes to the connection must be made from EMS, not from FortiClient. When FortiClient is connected to EMS, FortiClient settings are locked, so the endpoint user cannot change any configuration.

Integrated Mode With Security Fabric

- FortiClient EMS provides FortiClient endpoint provisioning
- FortiClient endpoints connect FortiClient Telemetry:
  - To EMS to receive configuration information from FortiClient EMS
  - To FortiGate to participate in the Fortinet Security Fabric
- FortiGate also receives dynamic endpoint group lists from EMS
  - To build dynamic firewall policies
- FortiClient only register to a FortiGate if:
  - FortiClient is registered to EMS
  - FortiClient has received a gateway list from EMS
  - EMS has allocated a Fabric Agent license seat to endpoint
- Compliance enforcement is supported only with FortiOS version 6.2.0 or later



FORTINET

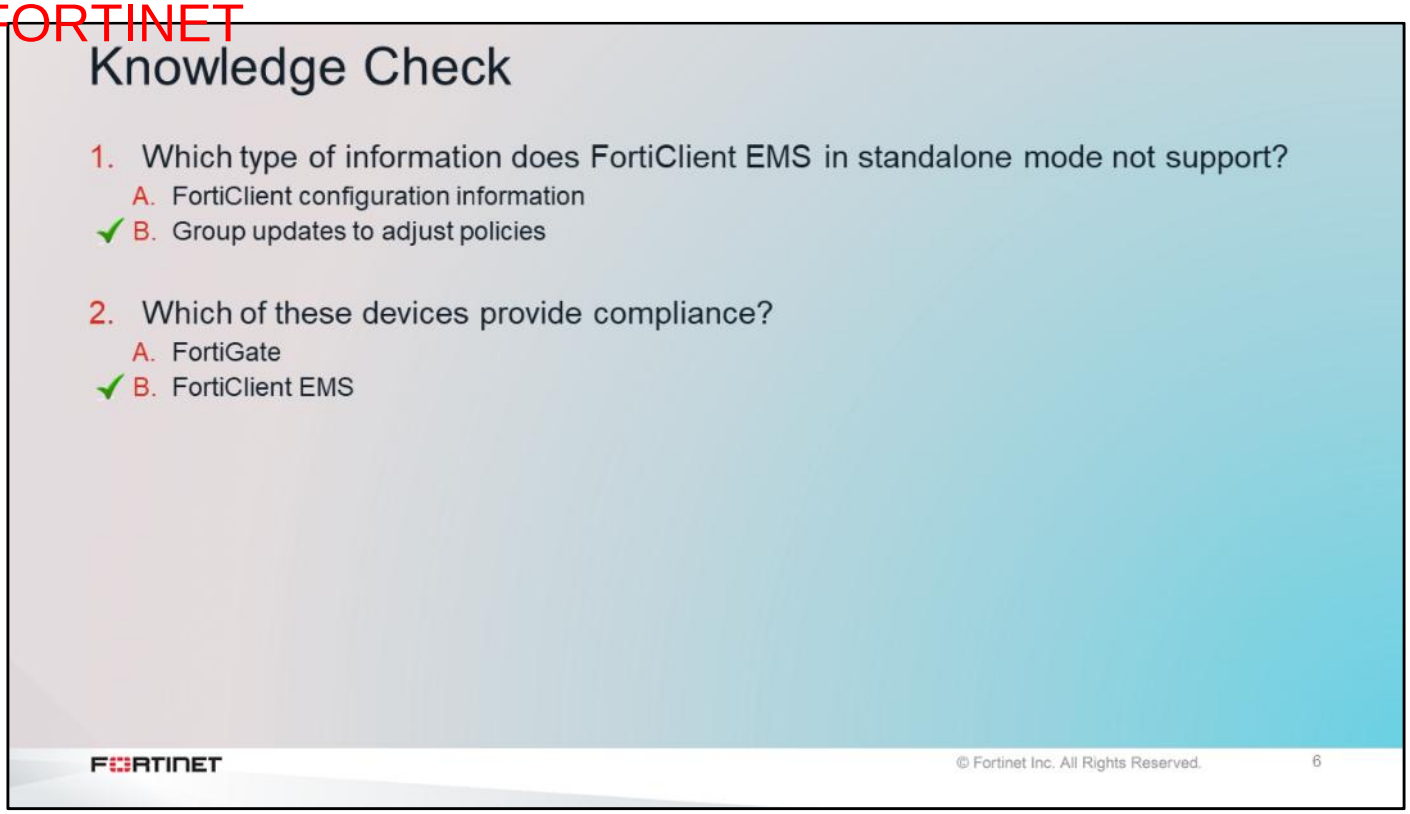
 5

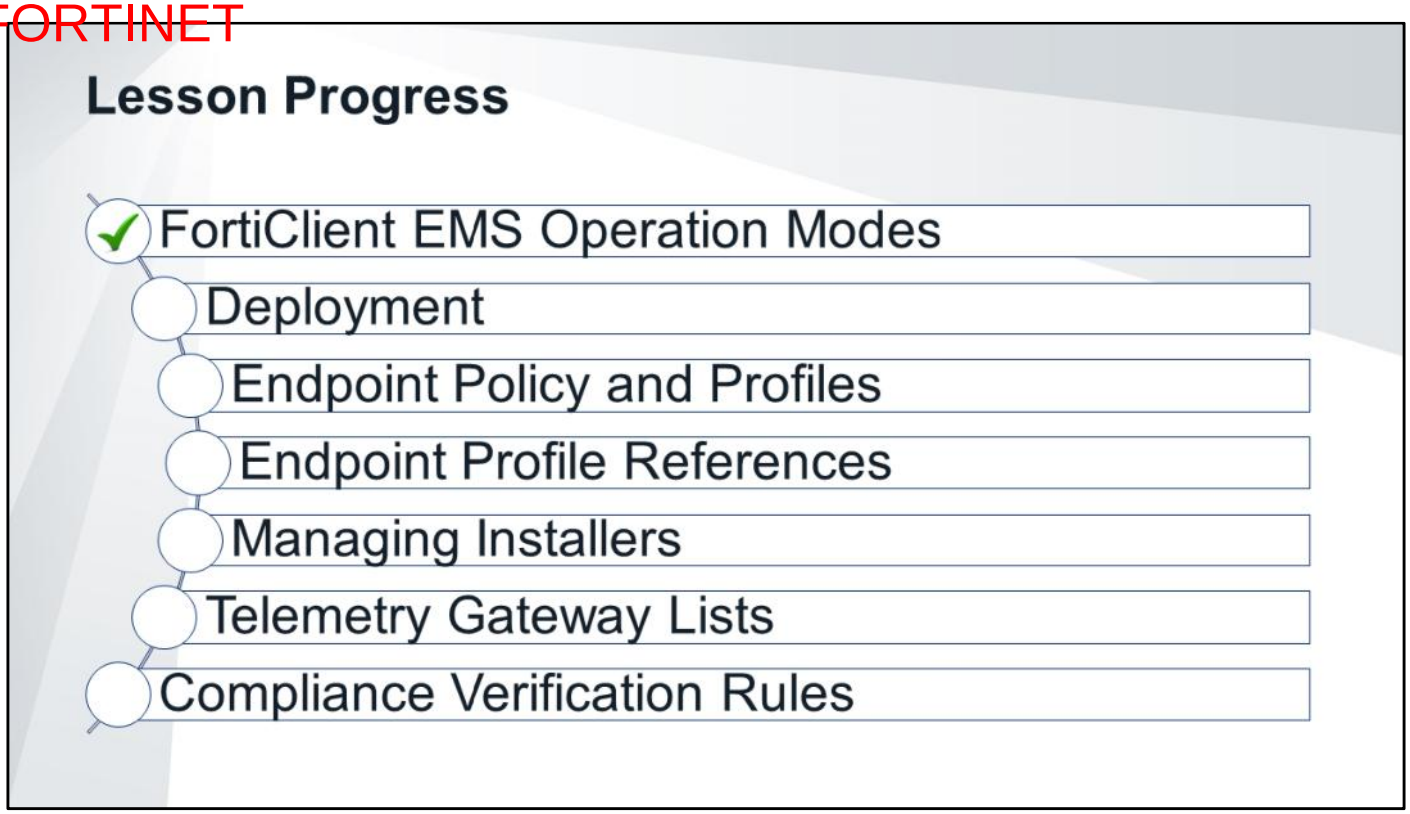
You can integrate FortiGate with FortiClient EMS. In this scenario, FortiClient Telemetry connects to EMS to receive a profile of configuration information as part of an endpoint policy, and it connects to FortiGate to participate in the Fortinet Security Fabric. FortiGate can also receive dynamic endpoint group lists from EMS and use them to build dynamic firewall policies. EMS sends group updates to FortiOS, and FortiOS uses the updates to adjust the policies based on those groups. This feature requires FortiOS version 6.2.0 or a later.

FortiClient registers to a FortiGate only if all of the following are true:
- FortiClient is registered to EMS.
- FortiClient has received a telemetry gateway list from EMS.
- EMS has allocated a Fabric Agent license seat to the endpoint. A Fabric Agent license is required to register to the FortiGate.

Depending on the EMS compliance verification rules and policies configured in FortiOS, the FortiClient endpoint may be blocked from accessing the network. The EMS administrator can adjust the endpoint configuration so that the endpoint regains network access.

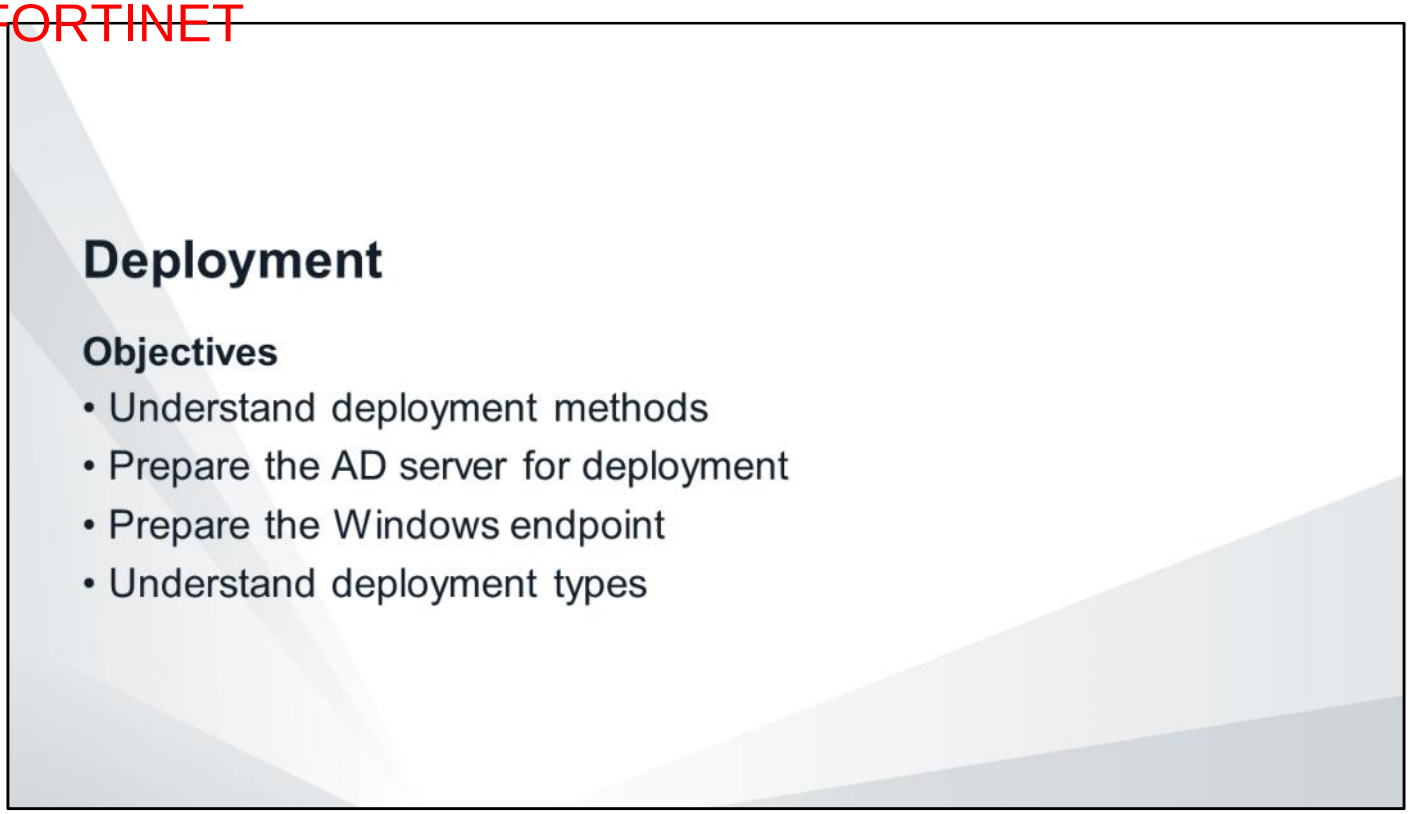
Please note that if you are using a version of FortiOS earlier than 6.2.0, FortiClient endpoints can connect to the Security Fabric, but compliance enforcement is not supported.





Good job! You now understand FortiClient EMS operation modes.

Now, you will learn about how to deploy FortiClient to endpoints.

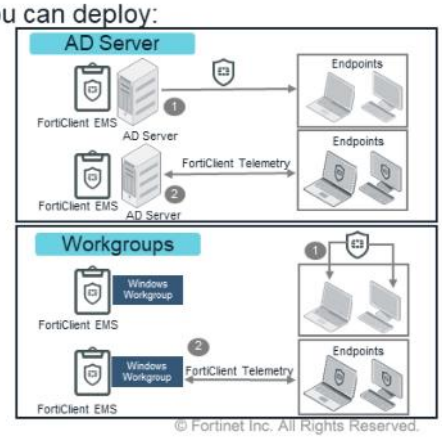


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in FortiClient deployment, you will be able to prepare Windows Active Directory (AD) server and endpoints, as well as implement different deployment types.

Deployment Methods

- You can add FortiClient to EMS:
  - Using an AD
  - Using workgroups
- AD:
  - You can deploy initial installation of Windows FortiClient but can not deploy macOS FortiClient
  - After installation endpoints are connected to EMS, you can deploy:
    - Upgrades
    - Removals
    - Replacement of FortiClient for Windows and macOS
- Workgroup:
  - You cannot deploy an initial installation
  - You can use workgroups to uninstall and update FortiClient on endpoints



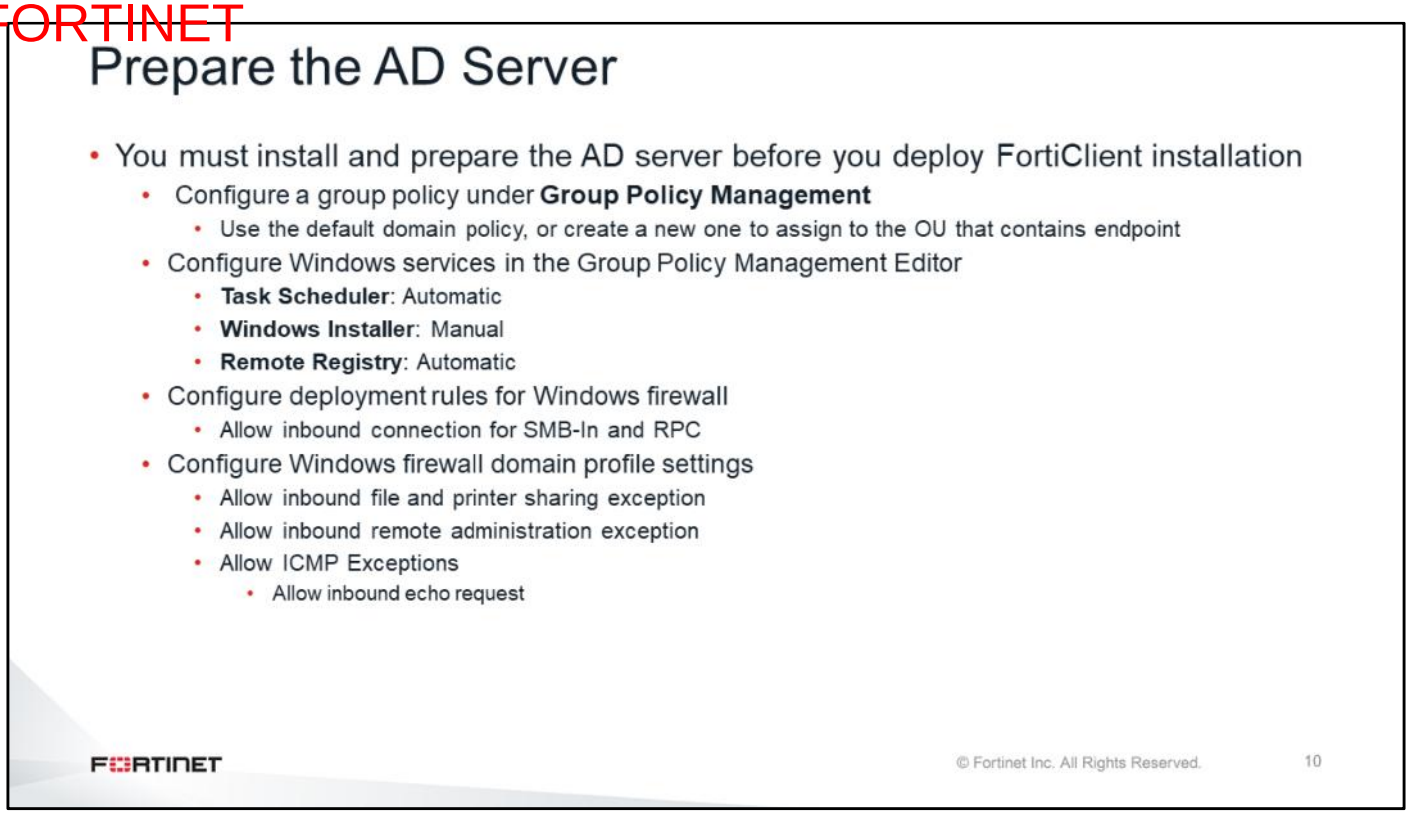
FORTINET

9

You can deploy FortiClient to endpoints using AD servers and workgroups. There are differences between using AD servers and workgroups.

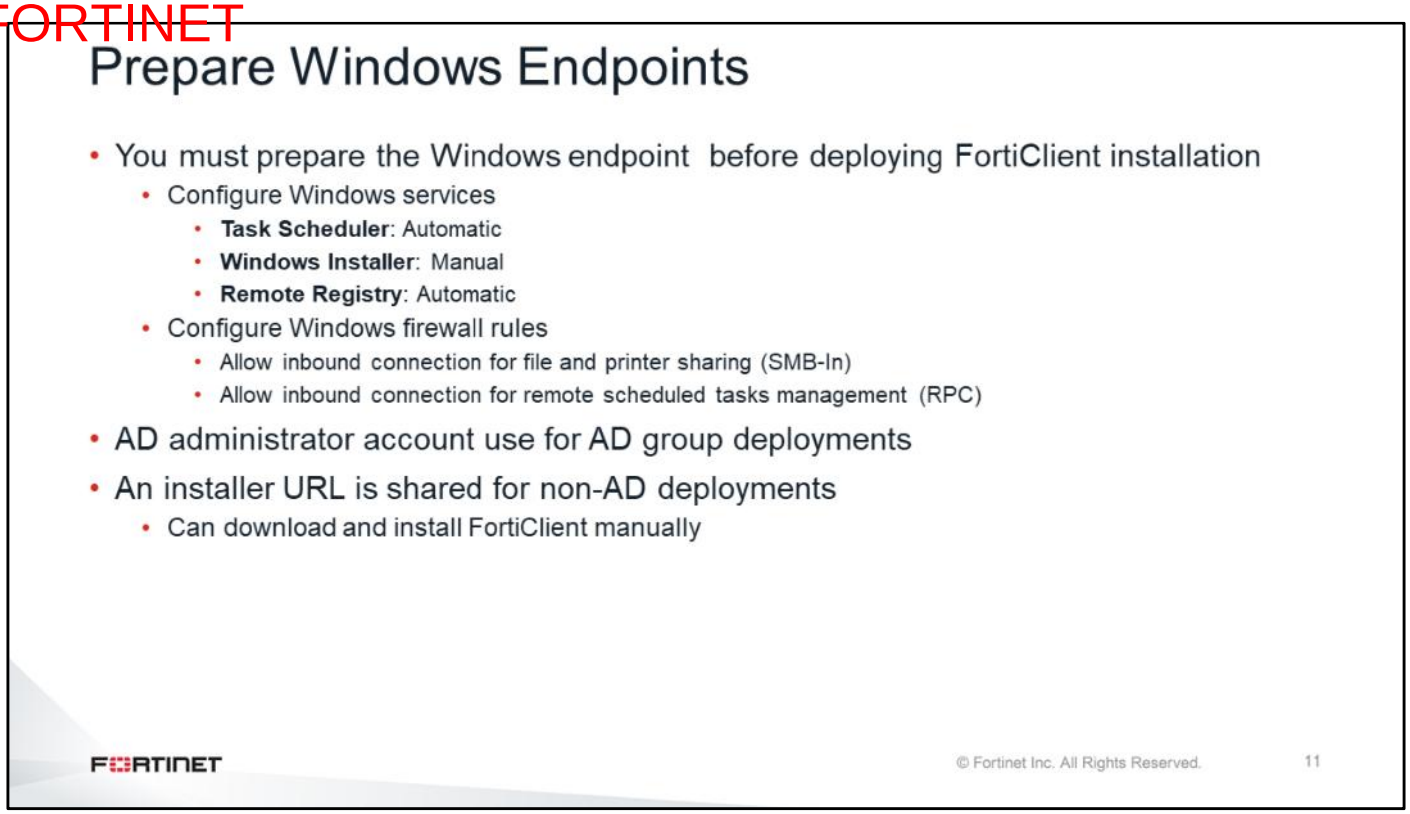
When using an AD server, you can deploy an initial installation of FortiClient (Windows) to endpoints, but you cannot deploy an initial installation of FortiClient (macOS). After FortiClient for Windows or macOS is installed on endpoints and endpoints are connected to FortiClient EMS, you can deploy upgrades, removals, and replacements of both FortiClient for Windows and macOS using AD servers.

When using workgroups, you cannot deploy an initial installation of FortiClient to endpoints. However, after FortiClient is installed on endpoints and endpoints are connected to FortiClient EMS, you can use workgroups to uninstall and update FortiClient on endpoints.



To deploy FortiClient from FortiClient EMS, you must prepare the AD server for deployment and deploy FortiClient on the endpoints. Before you can successfully deploy a FortiClient installation, ensure you install and prepare the AD server by following the steps that are shown on this slide.

Note that you cannot use FortiClient EMS to deploy an initial installation of FortiClient to endpoints (macOS and workgroup computers). However, after FortiClient is installed on endpoints, and the endpoints are connected to FortiClient EMS, you can use FortiClient EMS to uninstall and update FortiClient on endpoints.



You must enable and configure the following services on each Windows endpoint before FortiClient deployment:

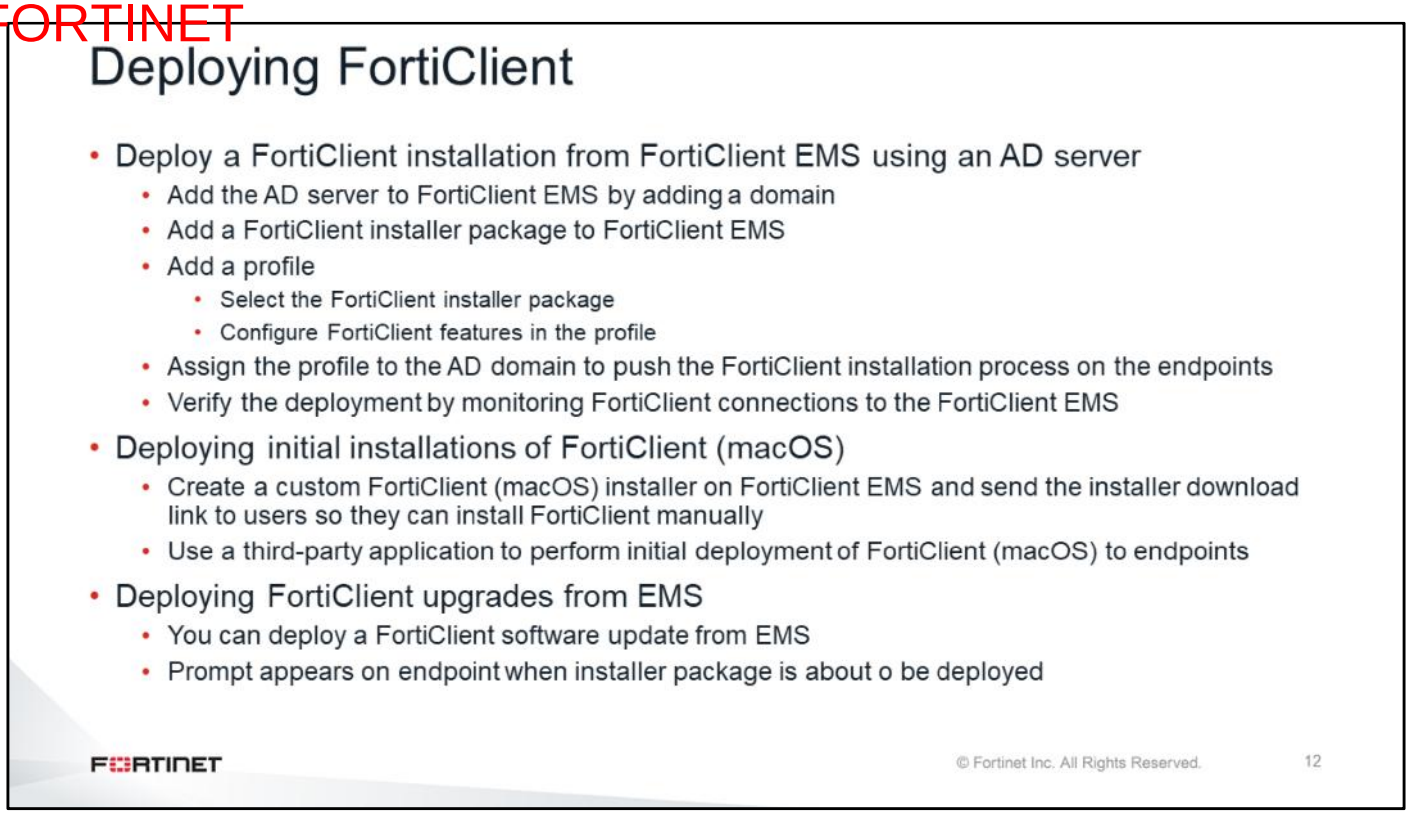
- **Task Scheduler**: Automatic
- **Windows Installer**: Manual
- **Remote Registry**: Automatic

The Windows firewall must allow SMB-in and RPC traffic for inbound connections.

For AD group deployments, an AD administrator account is required. For non-AD deployments, the installer URL can be shared with users, who can then download and install FortiClient manually. You can locate the installer URL in the **Manage Installers** pane.

Note that when you are adding endpoints using an AD domain server, FortiClient EMS automatically resolves endpoint IP addresses during initial deployment of FortiClient. FortiClient EMS can deploy FortiClient (Windows) to AD endpoints that do not have FortiClient installed, as well as upgrade existing FortiClient installations, if the endpoints are already connected to the EMS server.

You can execute `gpresult.exe /H gpresult.html` on any AD client to verify if you have an issue pushing the group policy to the endpoints.

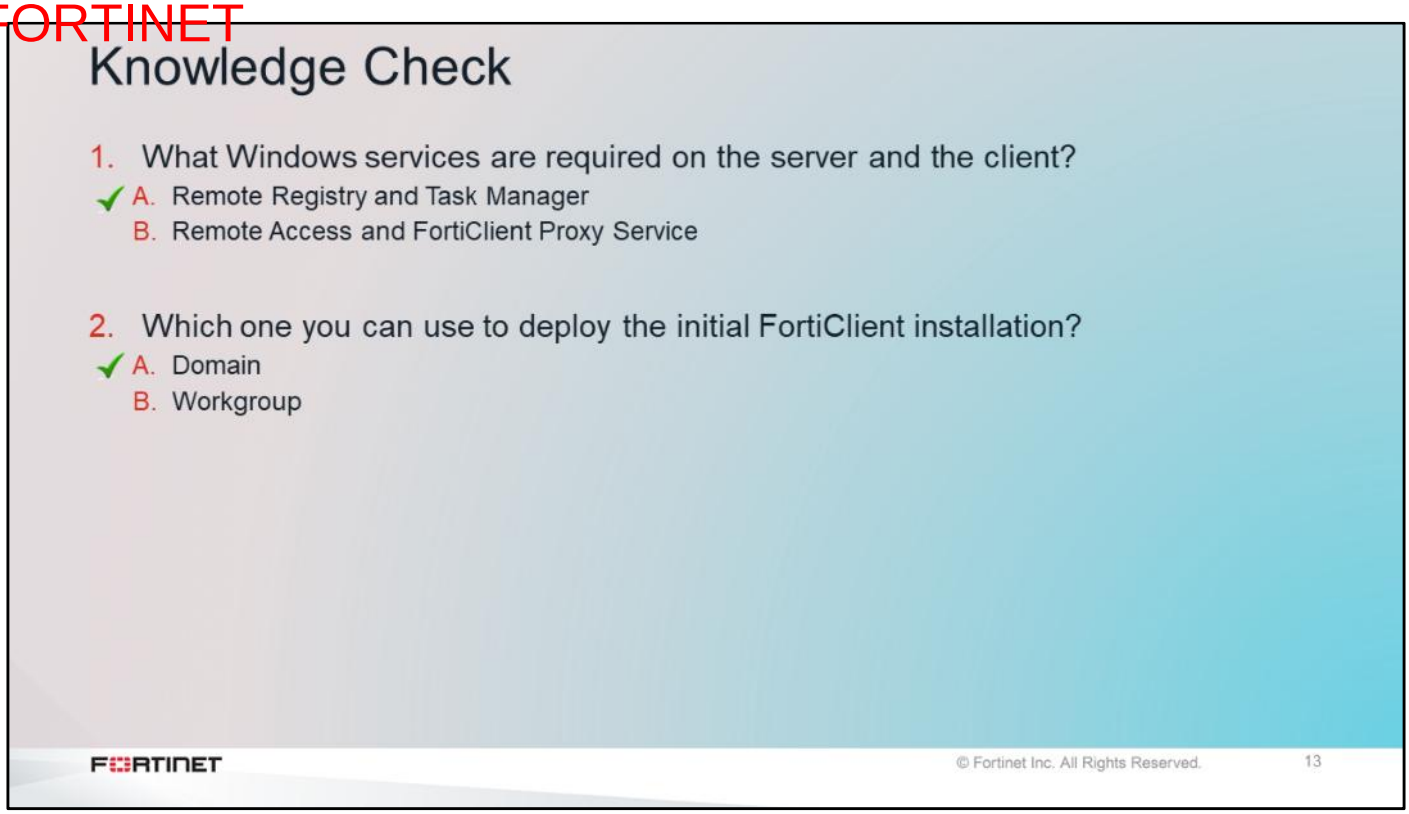


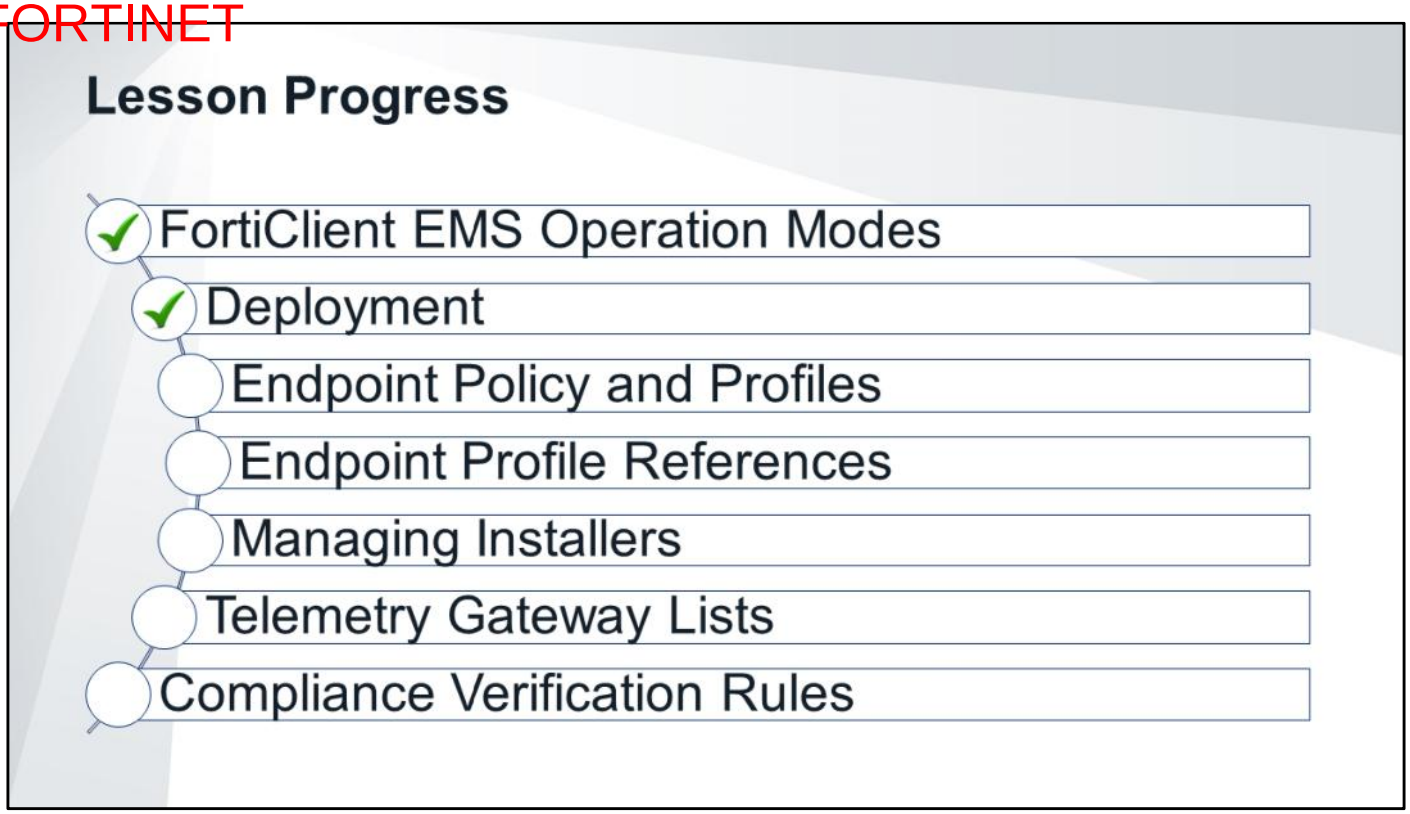
- Deploying FortiClient on Windows endpoints using an AD server: For successful deployment of FortiClient installation from FortiClient EMS using an AD server, you must prepare the AD server, add the AD server to FortiClient EMS as a domain, add an installer package to FortiClient EMS, add a profile (which includes the installer package and configured FortiClient features), and assign the profile to a branch of the AD domain to push the installation. You can verify the deployment by monitoring FortiClient connections to the EMS.

- Deploying initial installations of FortiClient on macOS: FortiClient EMS cannot be used to deploy initial installations of FortiClient (macOS). You can deploy an initial installation of FortiClient (macOS) by doing one of the options that are shown on this slide. After FortiClient (macOS) is installed on endpoints, and you have connected FortiClient Telemetry to FortiClient EMS, you can use FortiClient EMS to replace, upgrade, and uninstall FortiClient.

- Deploying FortiClient upgrades on endpoints running an older version: You can also deploy a FortiClient software update from EMS. A prompt appears on the FortiClient endpoint when an installer package is requested to be deployed. The prompt requests that the user do one of the following:
- **Upgrade Now**: If this option is selected, it performs the upgrade and automatically restarts your computer.
- **Upgrade Later**: If this option is selected, you can indicate the time to start the upgrade. The default is 8:00 PM. Your computer automatically restarts after the upgrade.

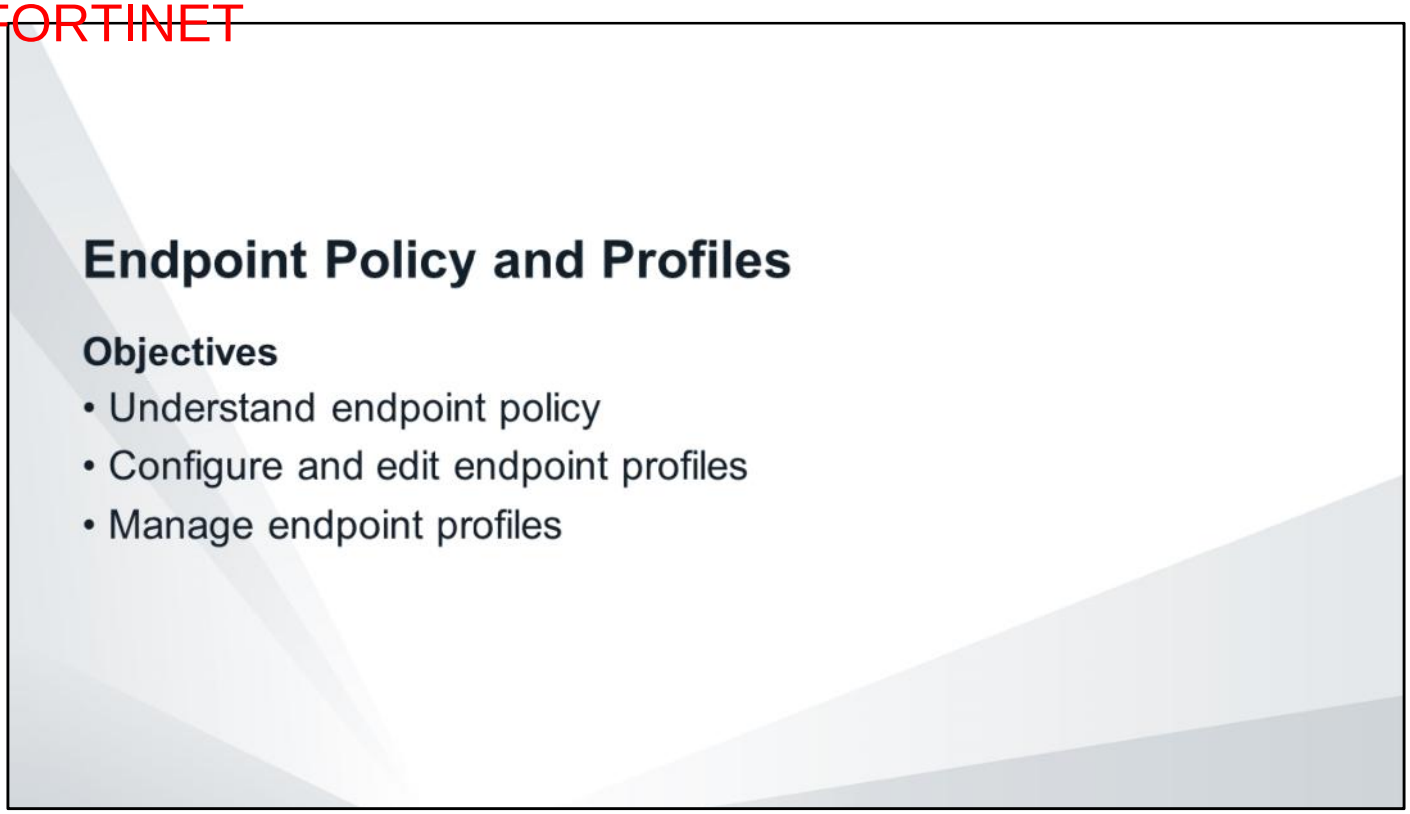
If no option is selected, the upgrade occurs, by default, at 8:00 PM. After FortiClient EMS uninstalls the previous version, it asks if the user wants to reboot now or reboot later.





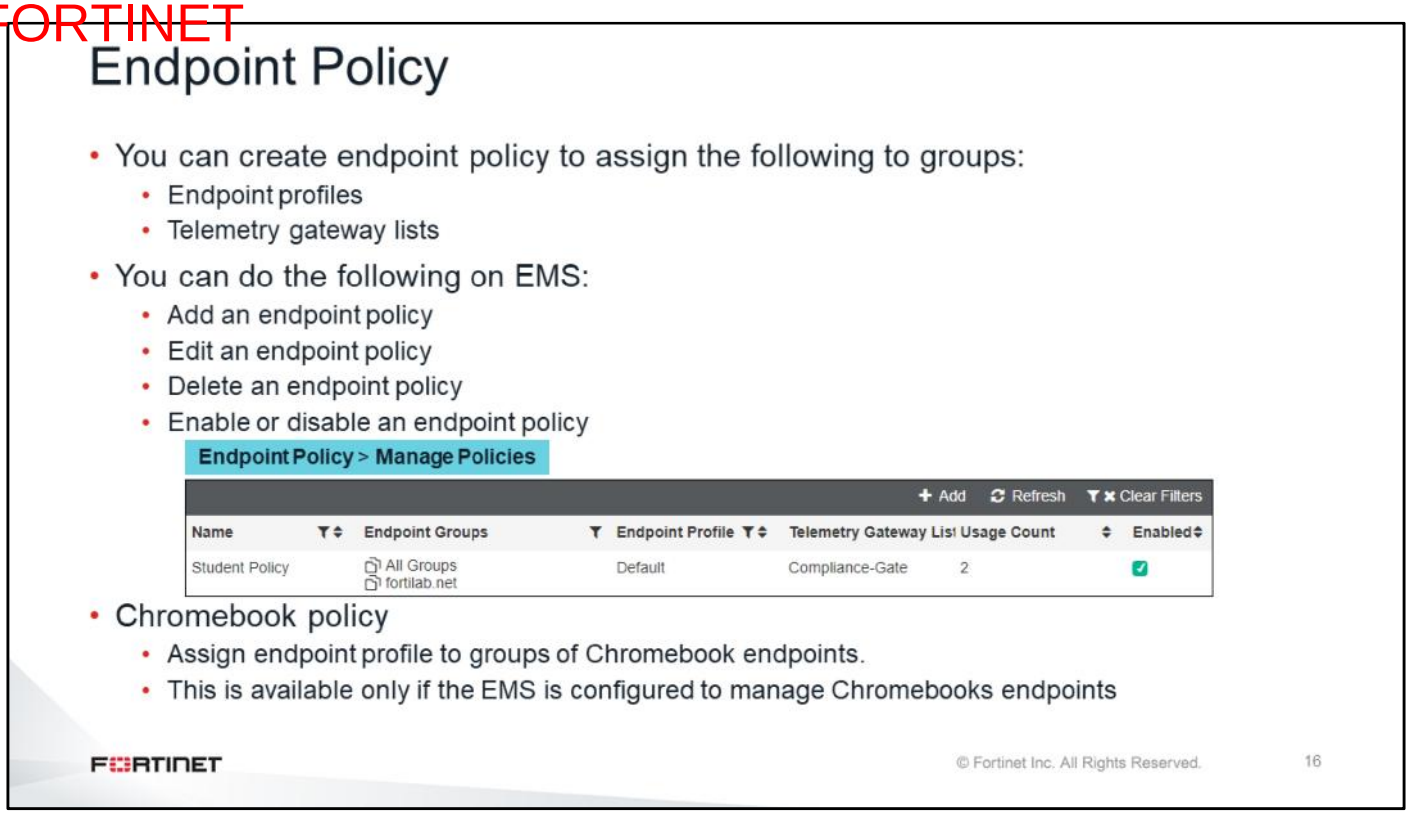
Good job! You now understand how to deploy FortiClient to endpoints.

Now, you will learn about endpoint policy and profiles.



After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in configuring, editing, assigning, and managing endpoint profiles, you will be able to use endpoint profiles to define the features installed on FortiClient endpoints.



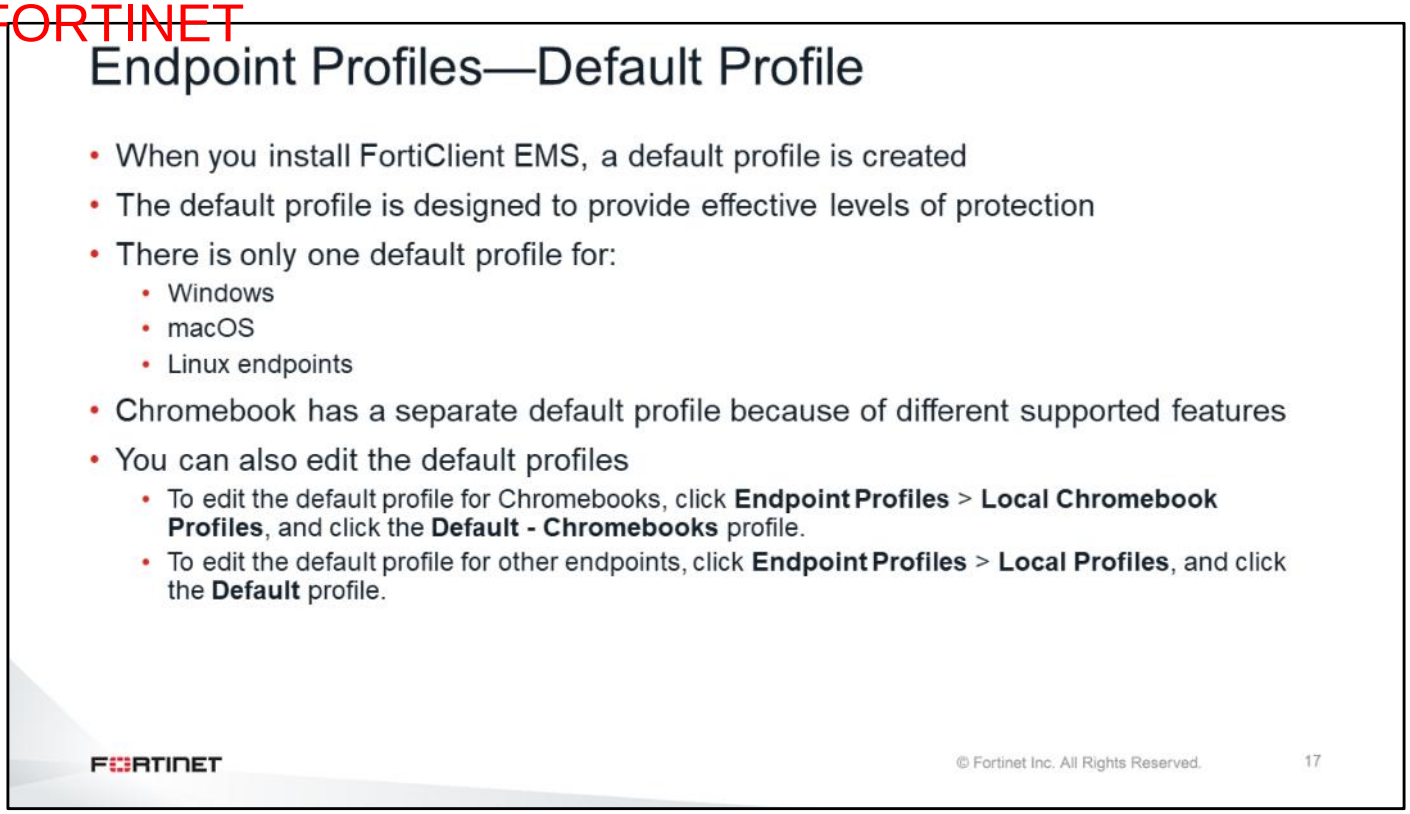
You can create endpoint policies to assign endpoint profiles and Telemetry gateway lists to groups of Windows, macOS, and Linux endpoints. The **Manage Policies** page provides a comprehensive summary of which endpoint policies are applied to which endpoint groups.

On the slide image, you can see that endpoints that belong to the domain fortilab.net group have the endpoint profile and Telemetry gateway list configured in the endpoint policy. EMS pushes these settings to the endpoint with the next Telemetry communication. In this example, endpoints in the fortilab.net group are applicable for the Student Policy. EMS applies only the Student Policy to the group.

You can add, edit, delete, and enable or disable policy in the **Manage Policies** page.

You can also create Chromebook policies to assign endpoint profiles and Telemetry gateway lists to groups of Chromebook endpoints. The **Manage Chromebook Policies** page provides a comprehensive summary of which policies are applied to which groups within the Google domain. This option is only available if the **EMS for Chromebooks Settings** option is enabled in EMS server.

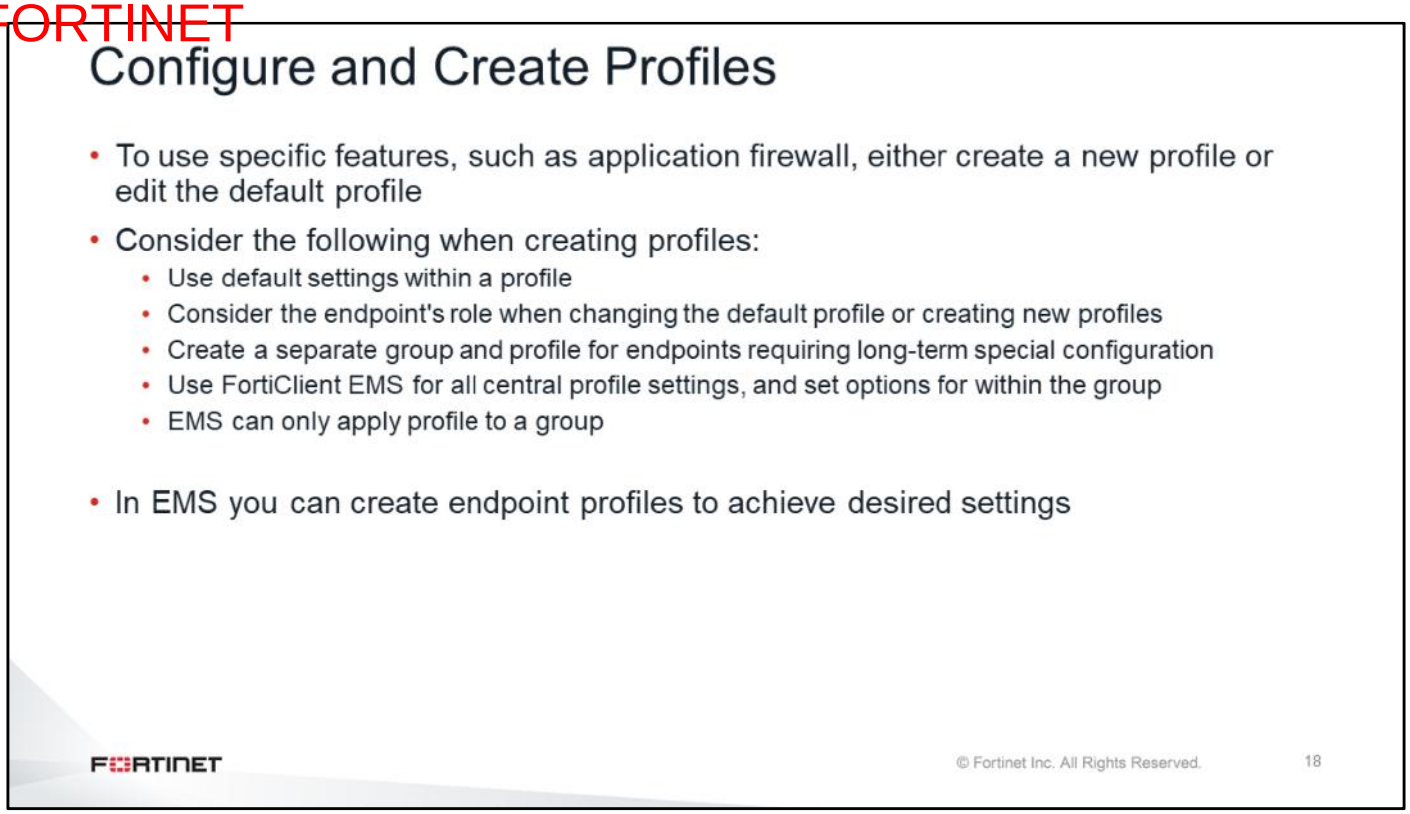
Chromebook policies function identically to Windows, macOS, and Linux endpoint policies, except that they are applied to Chromebook endpoints and can include only a Chromebook profile, not a Telemetry gateway list.



When you install FortiClient EMS, a default profile is created. By default, this profile is applied to any groups you create. The default profile is designed to provide effective levels of protection. There are separate default profiles for Windows, macOS, and Linux endpoints and for Chromebook endpoints.

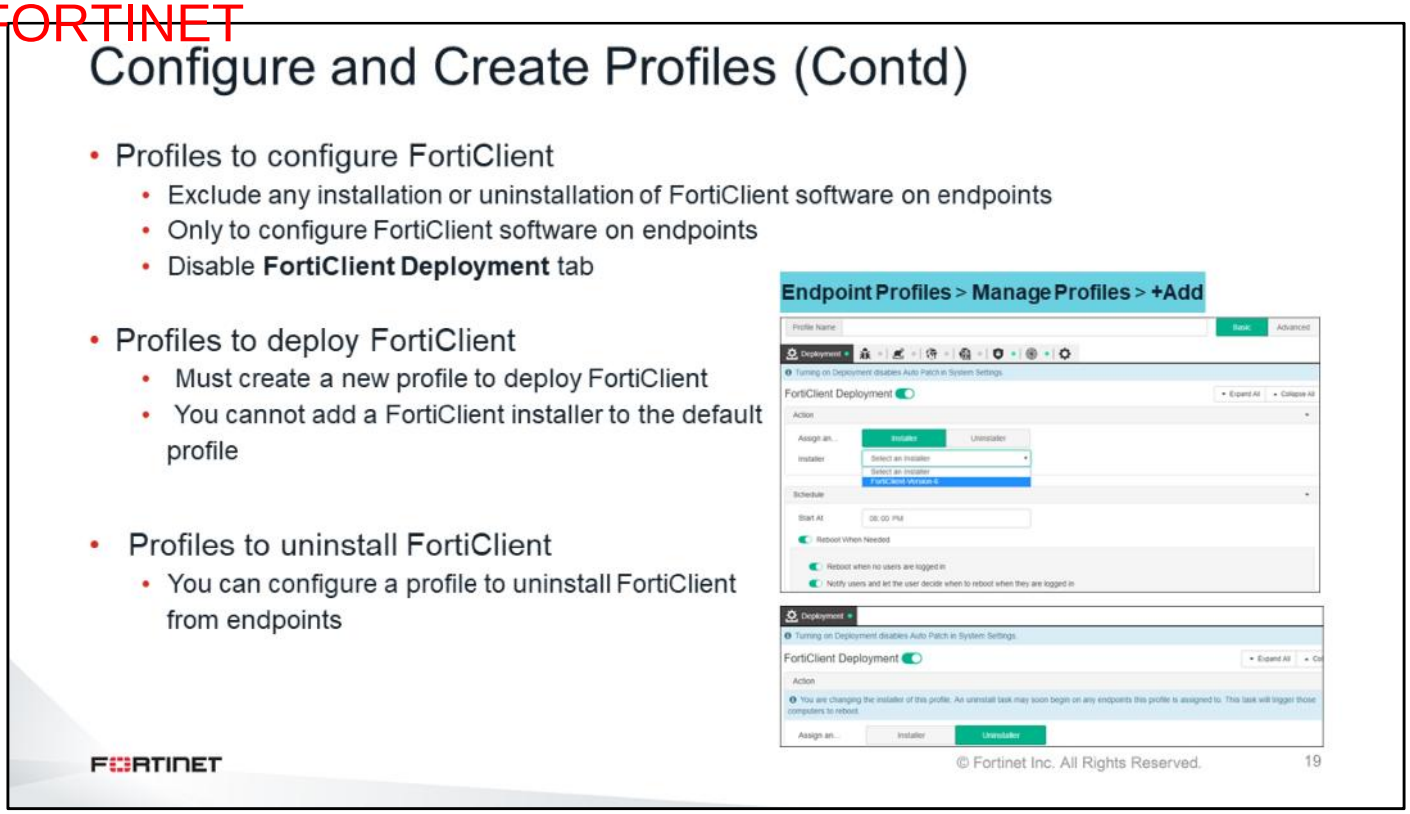
You can create and configure separate profiles for Windows, macOS, and Linux endpoints and for Chromebook endpoints. You can also edit the default profiles as shown on this slide.

You can edit, to add, or remove settings in the default profile. You can also revert to the default settings by clicking **Revert to Default**.



The default profile is designed to provide effective levels of protection. To use specific features, such as application firewall, create a new profile or edit the default profile.

Note that an individual FortiClient must belong to a group before the settings can be pushed to them.

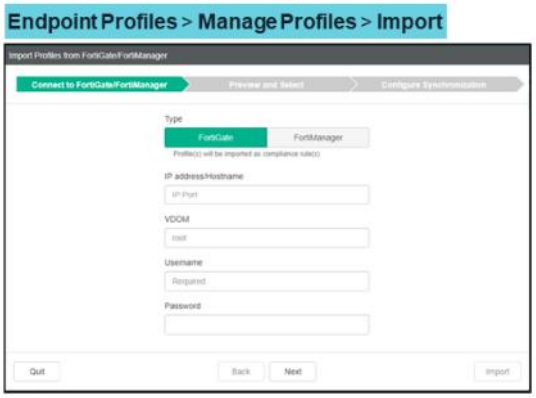


You can create endpoint profiles to achieve desired settings, such as:

- Profiles to configure FortiClient: This type of profile excludes any installation or uninstallation of FortiClient software on endpoints, and is used to configure FortiClient software on endpoints.
- Profiles to deploy FortiClient: You must create a new profile to deploy FortiClient to endpoints because you cannot add a FortiClient installer to the default profile. You must also add FortiClient installers to FortiClient EMS before you can select the installers in a profile. The selected FortiClient installer in a profile controls which tabs are displayed for configuration in the profile. Only the tabs for the features in the selected installer are displayed for configuration in the profile. For example, if the installer includes only the VPN feature, only the **VPN** tab is displayed for you to configure. The **System Settings** tab is always displayed. You can disable a feature included in the installer, then enable it later in the profile.
- Profiles to uninstall FortiClient: You can also configure a profile to uninstall FortiClient from endpoints. You must create a new profile for this configuration. You cannot use the default profile to uninstall FortiClient from endpoints.

Endpoint Profiles—Import Profiles

- Importing FortiGate web filter profiles
  - You can import a FortiClient web filter profile into EMS
- Importing FortiClient profiles from FortiManager
  - You can import web filter profiles from FortiManager into EMS



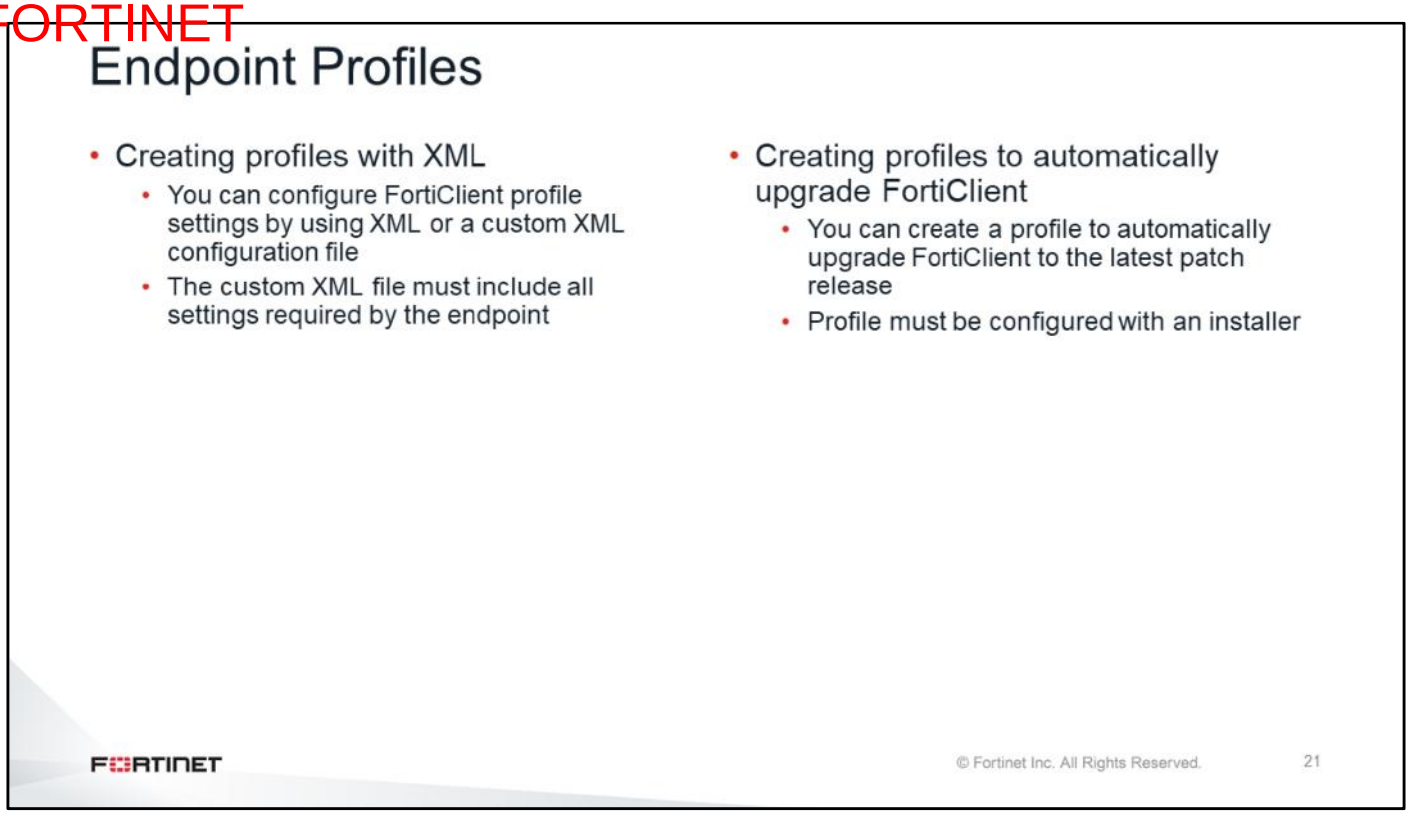
FORTINET

20

You can import a FortiClient web filter profile from FortiGate and FortiManager devices into EMS, then edit the profile in FortiClient EMS to add a FortiClient installer or other configuration details.

To import profiles successfully from FortiOS to FortiClient EMS, the HTTPS port on FortiGate and FortiManager must be open.

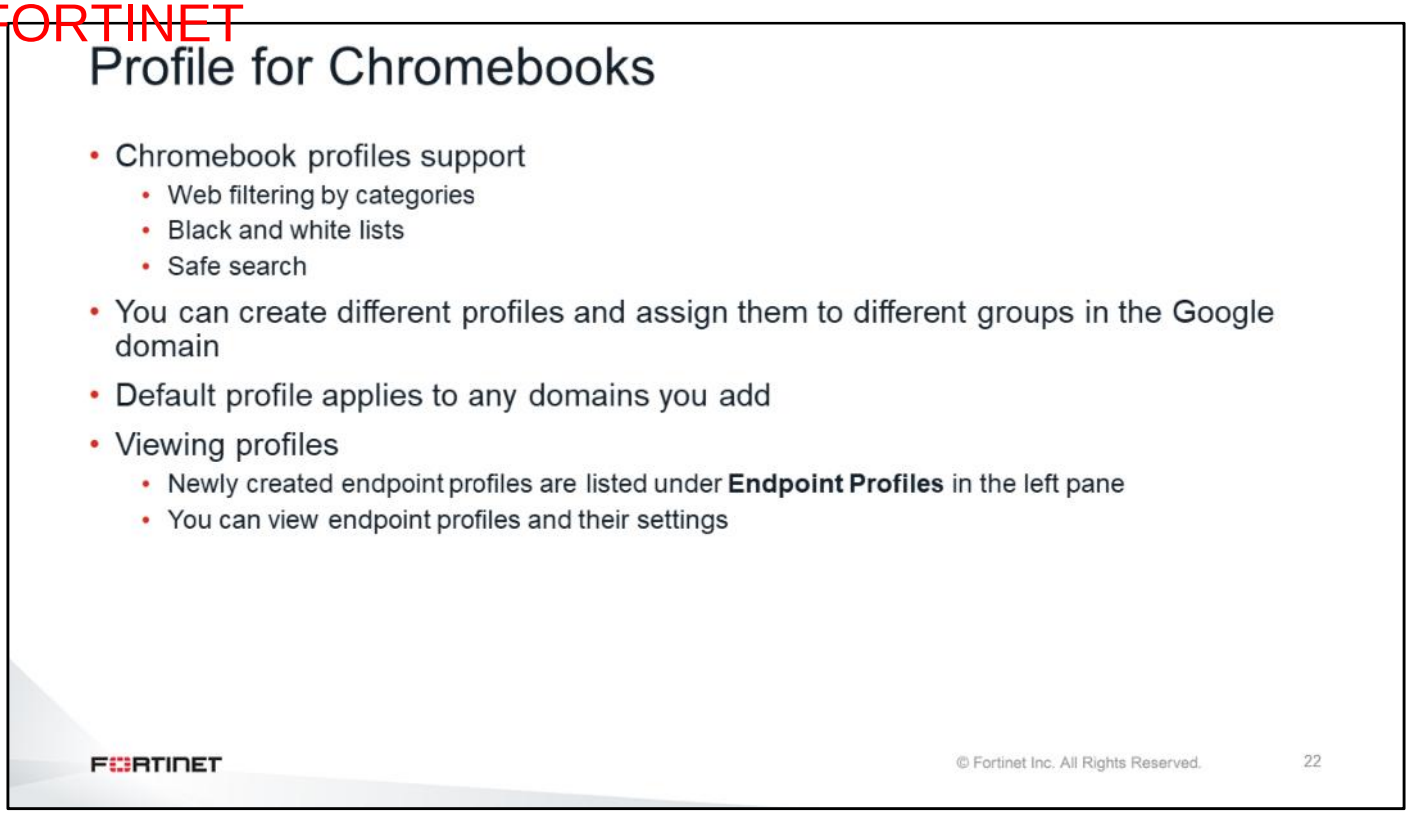
You need the IP address and port number of the FortiGate or FortiManager device from which the profile is being imported. You also need a VDOM name from the FortiGate or FortiManager, if applicable; login username; and password to connect.



You can configure FortiClient profile settings in FortiClient EMS by using XML or a custom XML configuration file. The custom XML file must include all settings required by the endpoint at the time of deployment.

Creating profiles to automatically upgrades the FortiClient. You can create a profile to automatically upgrade FortiClient to the latest patch release. The profile must be configured with an installer that meets the following requirements:

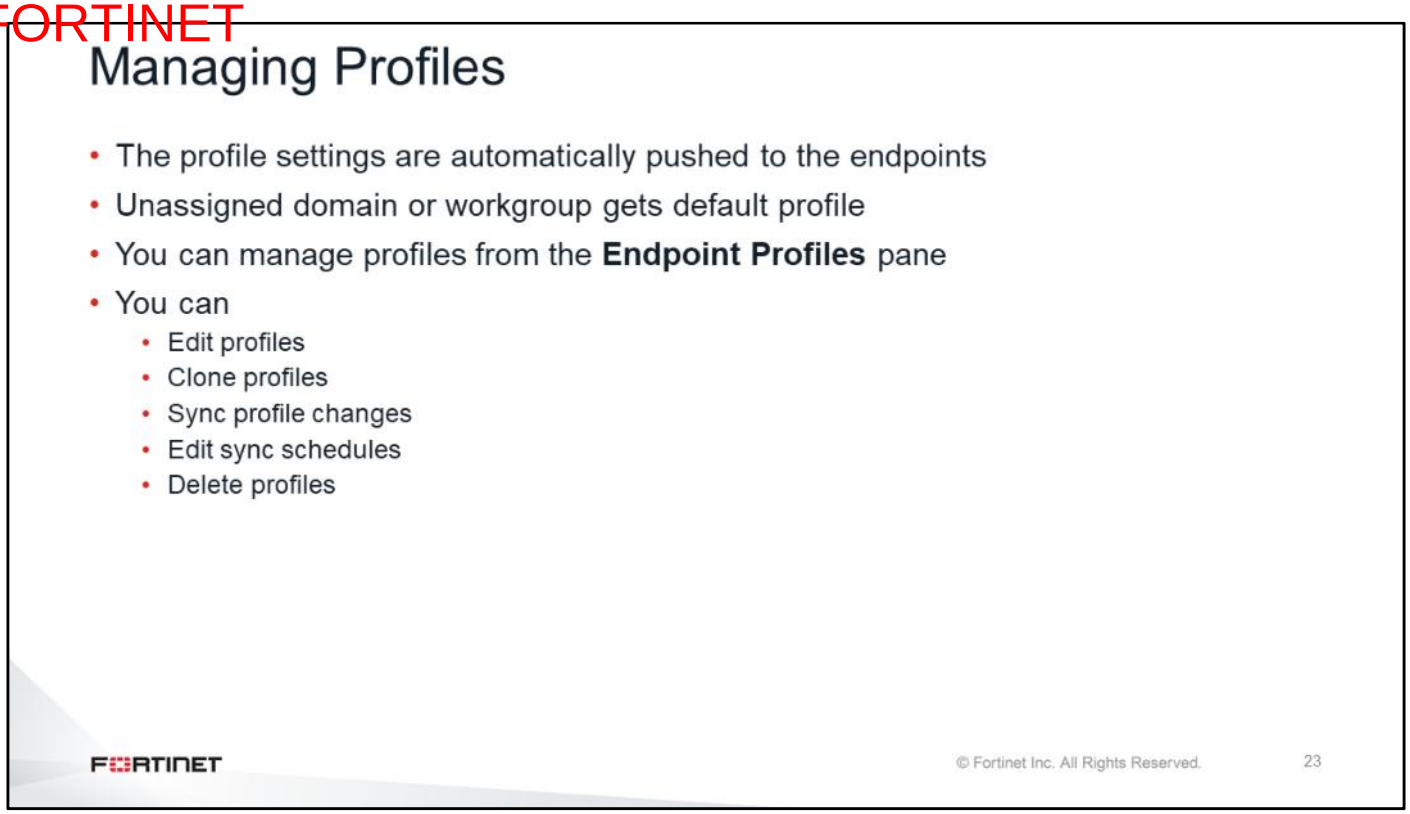
- The FortiClient installer was created in FortiClient EMS 1.2.0 or later.
- The FortiClient installer was created with the latest FortiClient version available for selection in FortiClient EMS at the time the installer was created.
- The FortiClient installer was created with the **Keep software updated to the latest patch release** option enabled.



Chromebook profiles support web filtering by categories, black and white lists, and safe search. You can create different profiles and assign them to different groups in the Google domain. When you install FortiClient EMS, a default profile is created. This profile is applied to any domains you add to FortiClient EMS.

The search engine provides a safe search feature that blocks inappropriate or explicit images from search results. The safe search feature helps block most adult content. FortiClient EMS supports safe search for most common search engines, such as Google, Yahoo, and Bing.

The profile in FortiClient EMS controls the safe search feature.

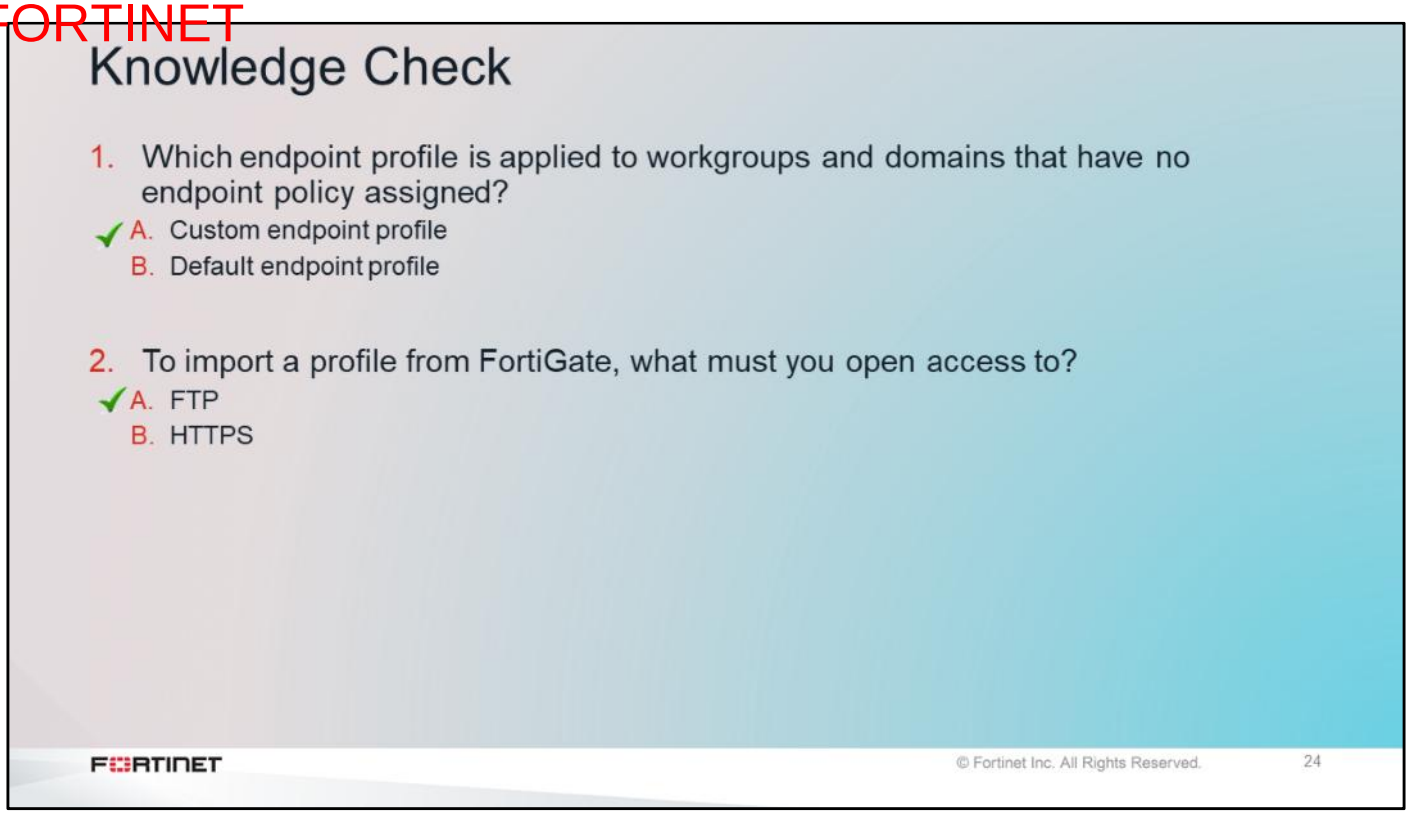


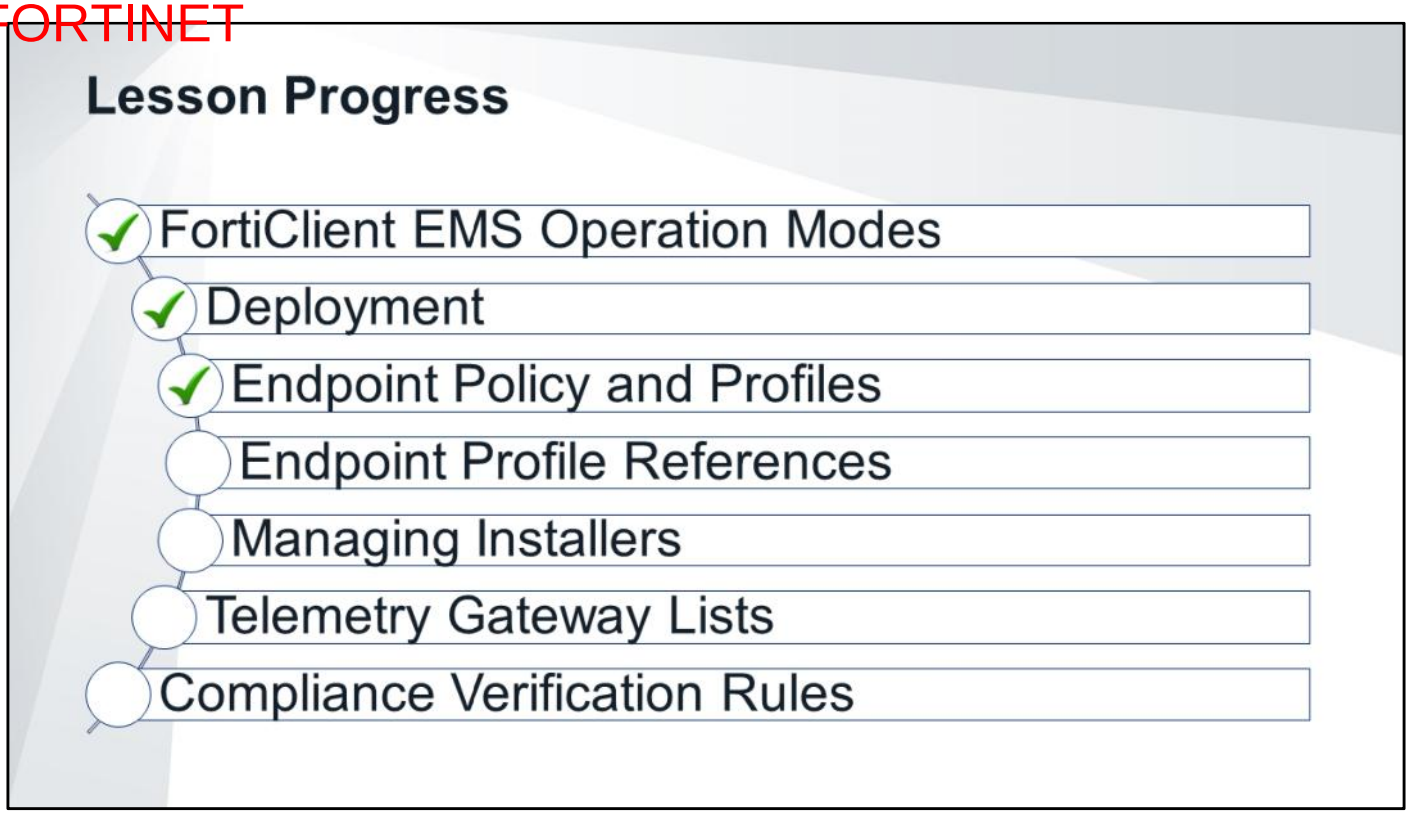
When you assign the profile using endpoint policy to domains or workgroups, the profile settings are automatically pushed to the endpoints in the domain or workgroup. If you do not assign a profile to a specific domain or workgroup, the default profile is automatically applied. After editing an existing profile assigned to endpoints or domains, the changes are also automatically pushed to the endpoints or Chromebooks when you save the profile.

When you clone a profile, all the content displays in the content pane, and you can save the cloned profile with a new name.

For profiles imported from FortiGate or FortiManager, you can manually sync profiles so they are updated with the latest changes from the FortiGate or FortiManager device that they were imported from. You can also edit the sync schedule time.

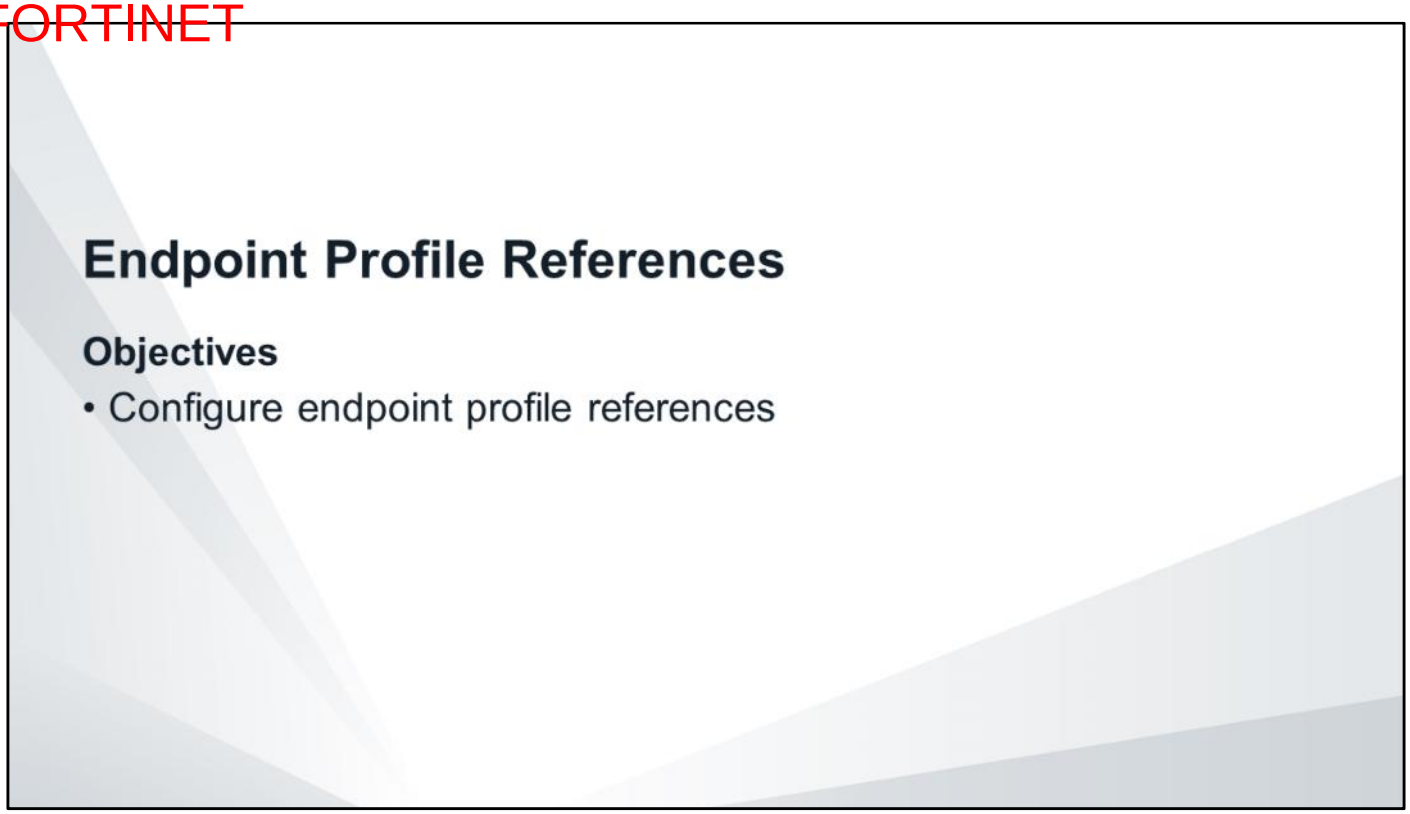
You can also delete any newly created profile. But note that you cannot delete the default profile and *not* the assigned profiles.





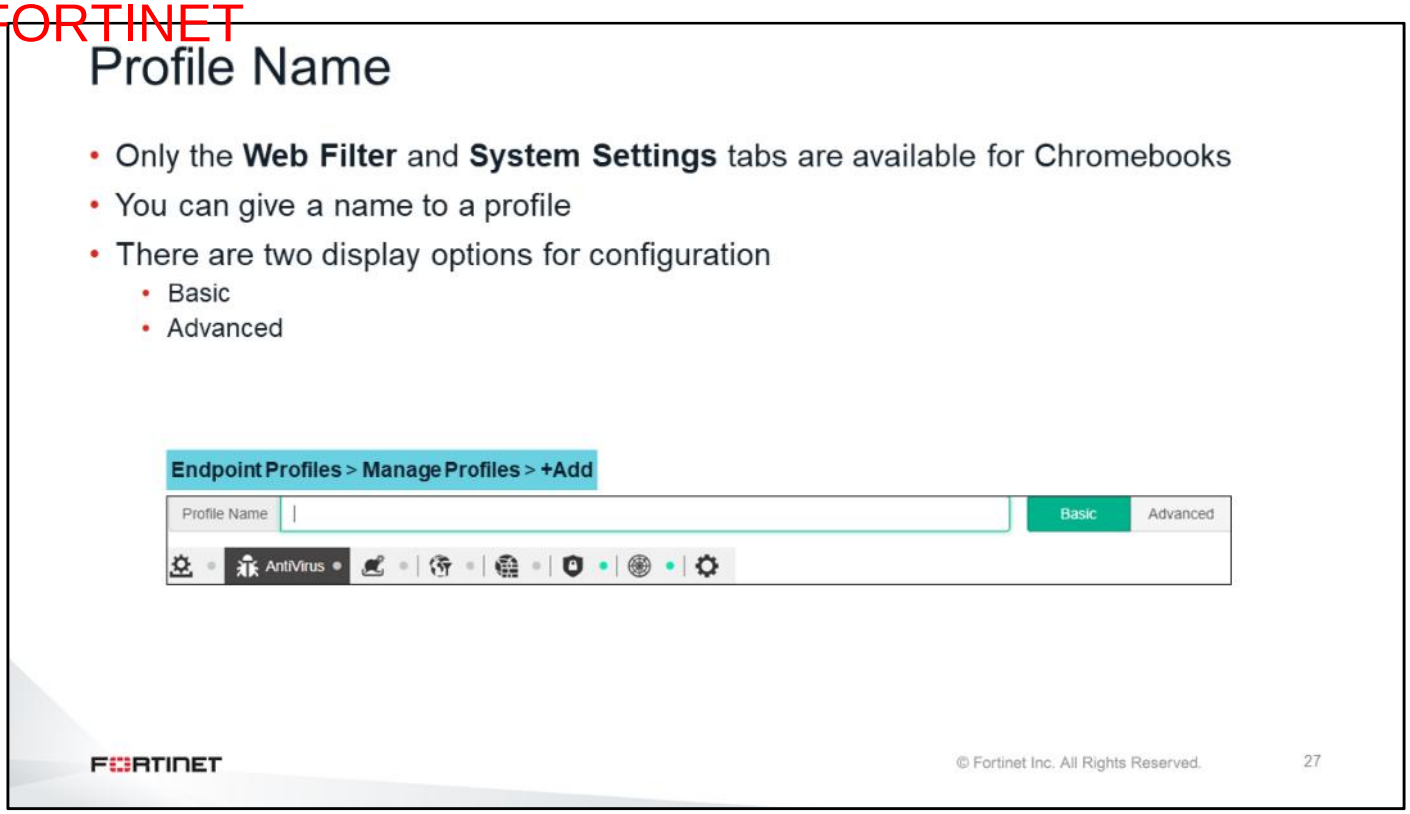
Good job! You now know how configure endpoint policy and manage endpoint profiles.

Now, you will learn about endpoint profile references.



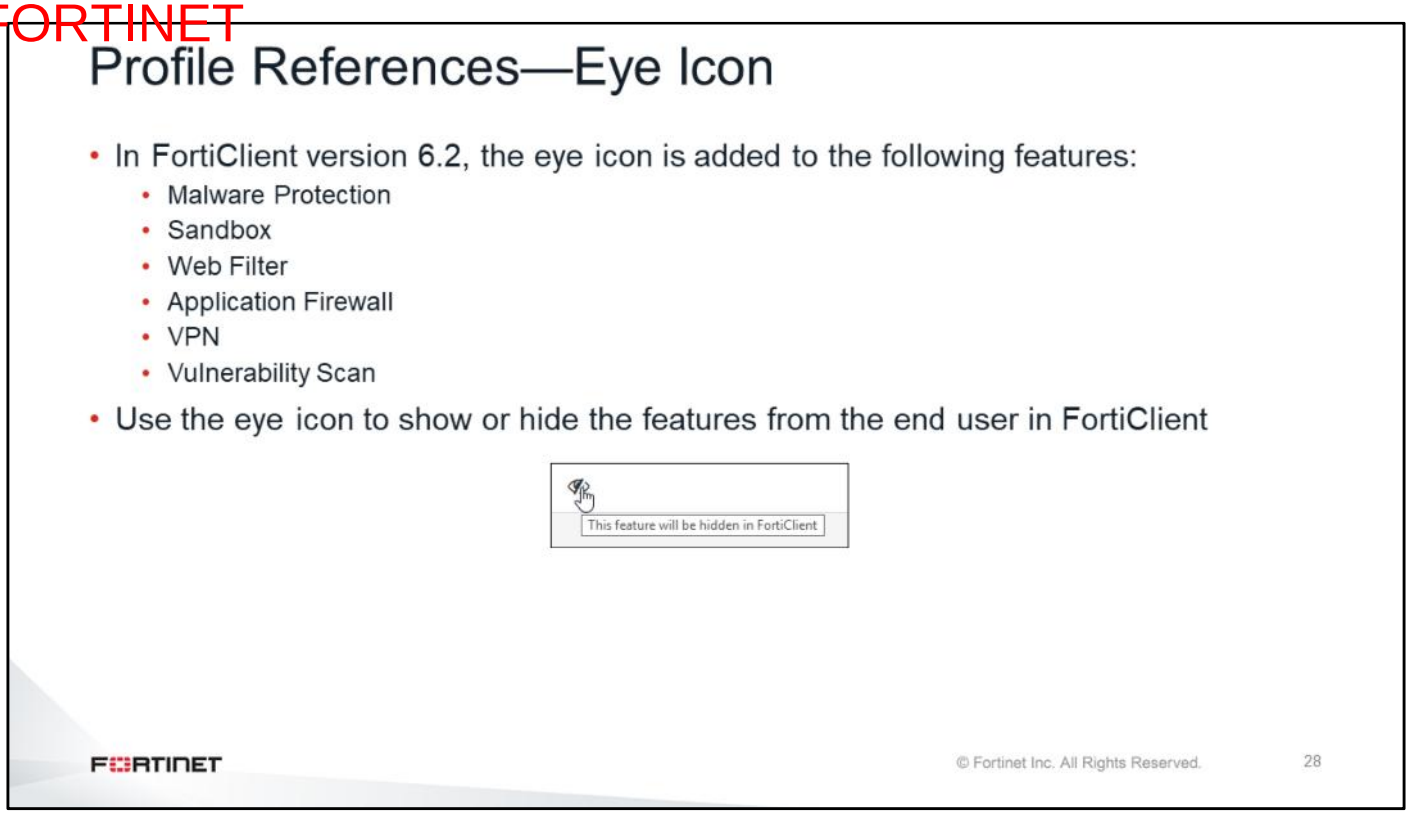
After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence in configuring endpoint references, you will be able to implement the settings required to use endpoint references in your network.



For Chromebooks, only the **Web Filter** and **System Settings** tabs are available. All other tabs are exclusive to Windows, macOS, and Linux endpoints.

The **Profile Name** allows you to enter a name and select a display option. The **Basic** display option shows all the GUI options. The **Advanced** display option enables the XML configuration tab to configure a profile using XML. This option is available only for Windows, macOS, and Linux profiles.



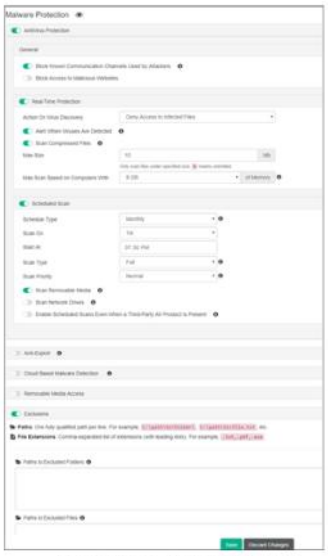
In FortiClient version 6.2, the eye icon is added to the following FortiClient features:

- Malware Protection
- Sandbox
- Web Filter
- Application Firewall
- VPN
- Vulnerability Scan

You can use the eye icon to show or hide the feature from the end user, in FortiClient. When you select hide, the feature will still run in the background, but the endpoint user can not see it. It is very useful when inspecting the traffic without the user's knowledge.

Malware Protection

- On the **Malware Protection** tab, you can enable **Antivirus Protection** to see the following sections and options:
  - **General Settings**
  - **Real-Time Protection**
  - **On Demand Scanning**
  - **Scheduled Scan**
  - **Anti-Exploit**
  - **Cloud Based Malware Detection**
  - **Removable Media Access**
  - **Exclusions**
  - **Other**



FORTINET

29

You can enable antivirus protection on FortiClient. Some options display only if you enable **Advanced**.

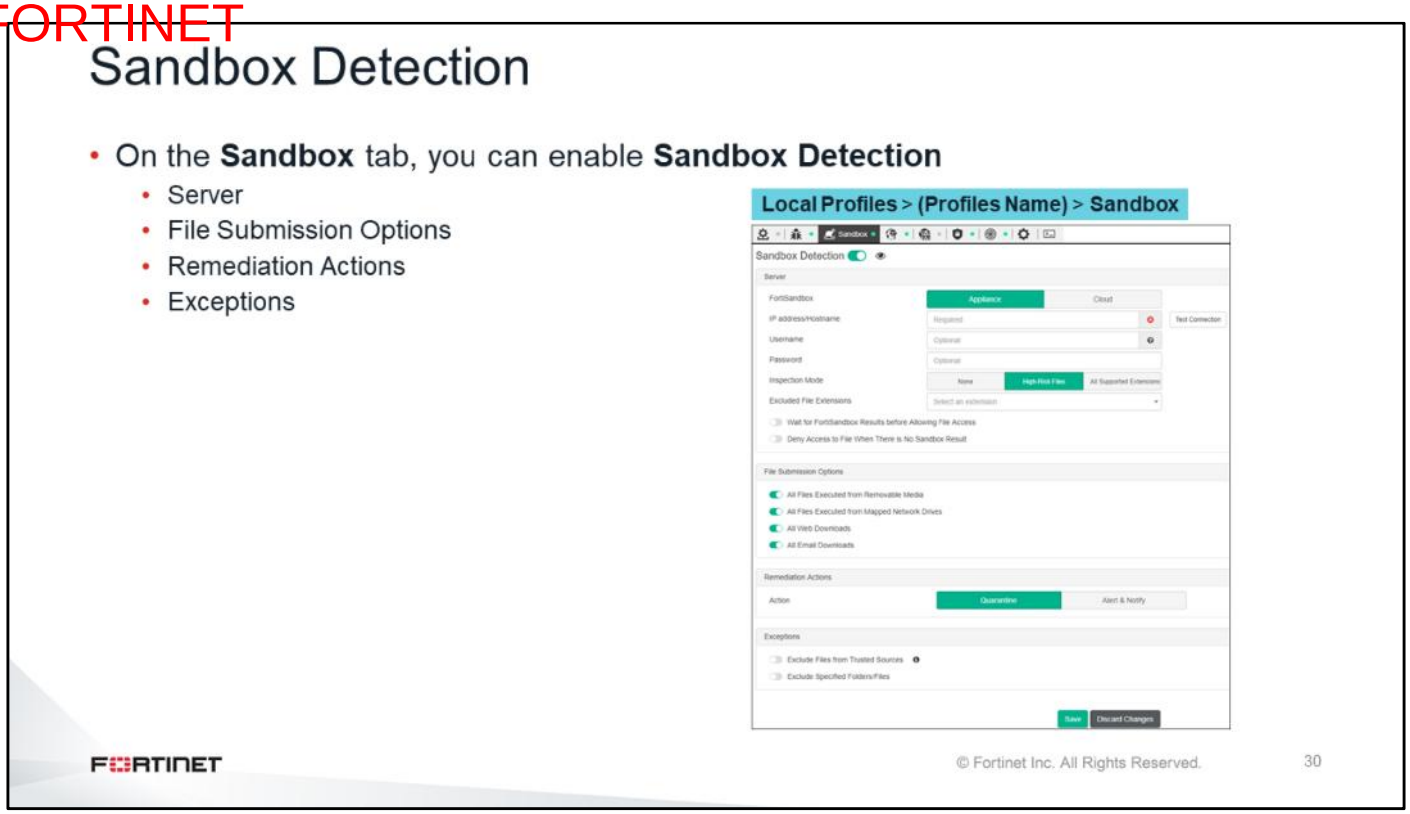
In the general settings, you enable or disable options that will block communication to known channels, block access to malicious websites, and identify malware and exploits using signatures from FortiSandbox.

In real-time protection settings**,** FortiClient can take different actions on virus discovery. You can also select file size and scan files accessed by a user or system process, such as read or write. On-demand scanning integrates FortiClient into the Windows Explorer' menu. You can pause scanning when a computer is running on battery power, and automatically submit suspicious files to FortiGuard for analysis. You can also select schedule type, scan type, and priority. You can also select removable media and network drives for scanning.

Antiexploit options enables the anti-exploit engine to monitor commonly used applications for attempts to exploit known vulnerabilities. You can exclude applications from anti-exploit detection and enable system tray notifications.

You can enable cloud-based malware outbreak detection. The cloud-based malware protection feature helps protect endpoints from high risk file types from external sources, such as the Internet or network drives, by querying FortiGuard to determine whether files are malicious.

You can also enable controlling access to removable media devices and file or folder exclusions from antivirus scanning. The **Other** option enables scanning for rootkits, adware, riskware, email, media on insertion, and advanced heuristics signature.

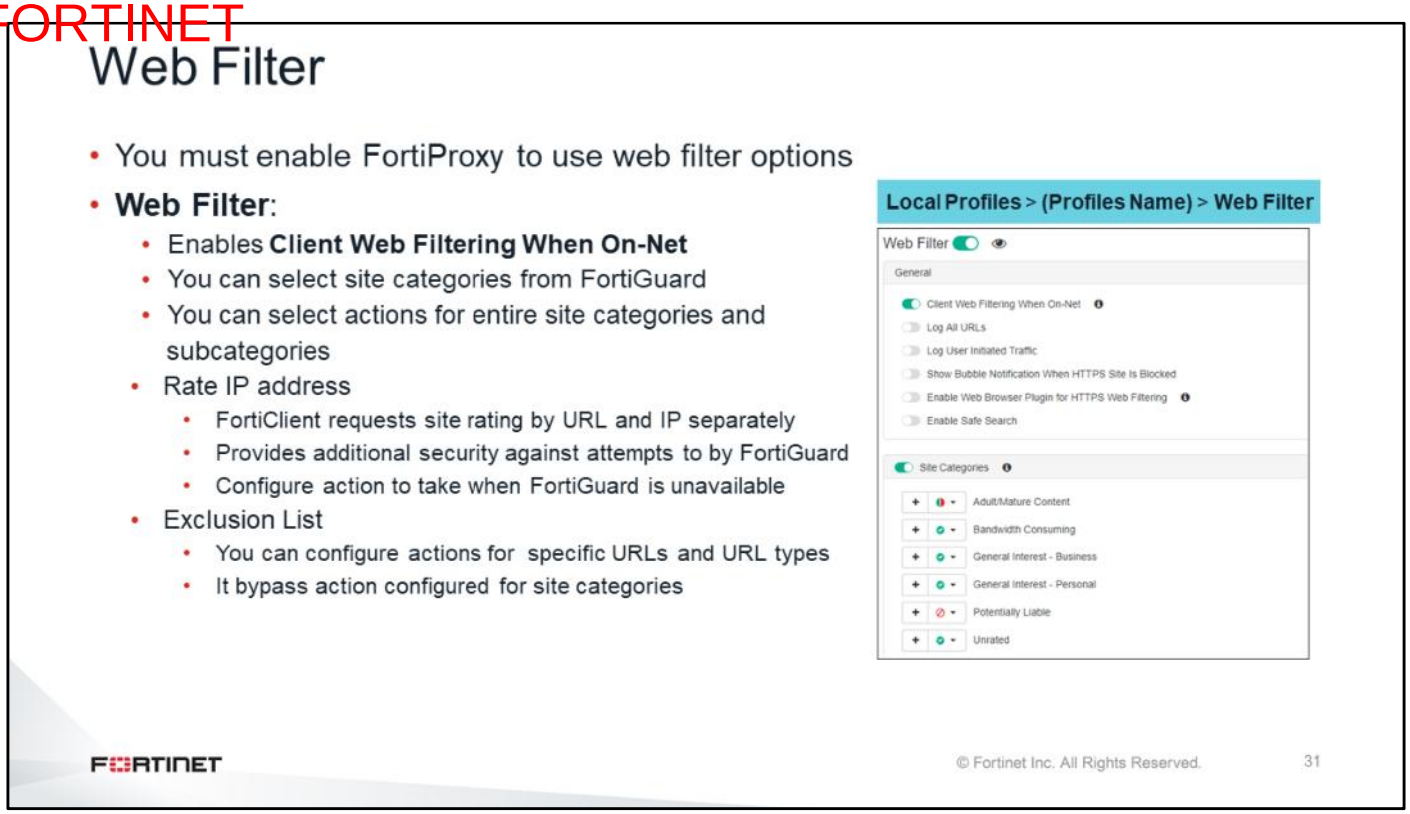


You can enable **Sandbox Detection** on the FortiClient. Some options display only if you enable **Advanced**.

The following options are available:

- **Server** allows you to select FortiSandbox in the network, and file access options based on results.
- In the **File Submission Options** section, you can select file resources like removable media, network drives, web downloads, and email downloads.
- **Remediation Actions** allows you to select the **Quarantine** or **Alert & Notify** action for infected files.
- **Exceptions** allows you to exclude files from trusted sources and specific files or folders.

In addition to configuring the options shown on this slide, you must also configure the connection to EMS on the FortiSandbox. On FortiSandbox, click **Scan** > **Devices**, and search for and authorize EMS using its serial number. You can find the EMS serial number on the **System Information** widget on the Dashboard.



The **Web Filter** tab enables web filtering options. For Windows, macOS, and Linux profiles, you must enable **FortiProxy (Disable Only When Troubleshooting)** on the **System Settings** tab to use the **Web** Filter.

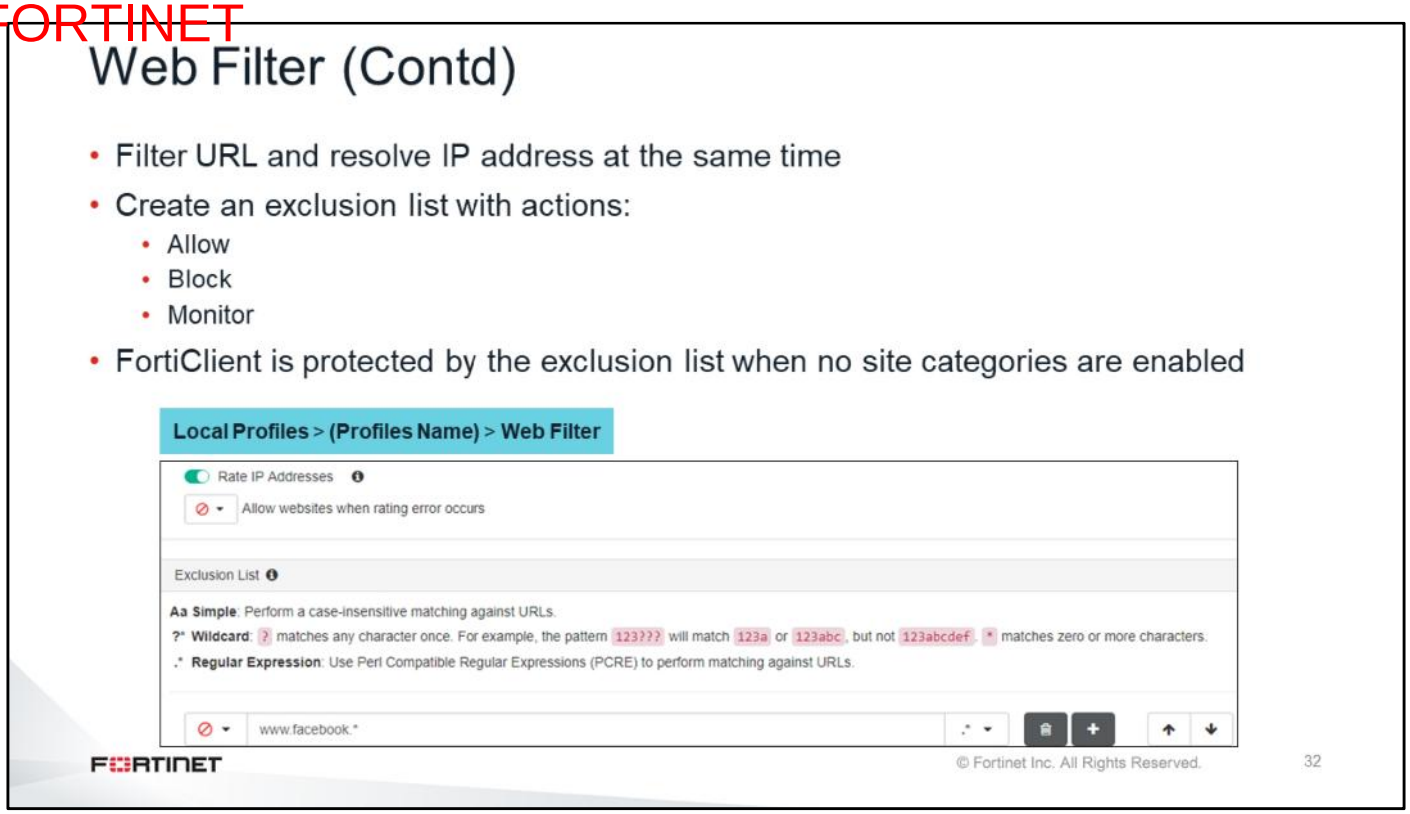
General setting includes **Client Web Filtering When On-Net** that allows FortiClient to perform web filtering even when it is on-net with FortiGate in the network also configured with a web filter profile. This option is available only for Windows and macOS profiles. This setting affects the **Block Access to Malicious Websites** setting in AntiVirus protection.

The **Log All URLs** enables logging for all URLs access by endpoint user. You can also enable **Log User Initiated Traffic** to include user information in web filtering logs.

The **Show Bubble Notification When HTTPS Site Is Blocked** enables the showing of a bubble notification when HTTPS site is blocked and select **Enable Web Browser Plugin for HTTPS Web Filtering** to improve detection and enforcement of Web Filter rules on HTTPS sites.

You can also enable the safe search option for search engines like Google search or YouTube.

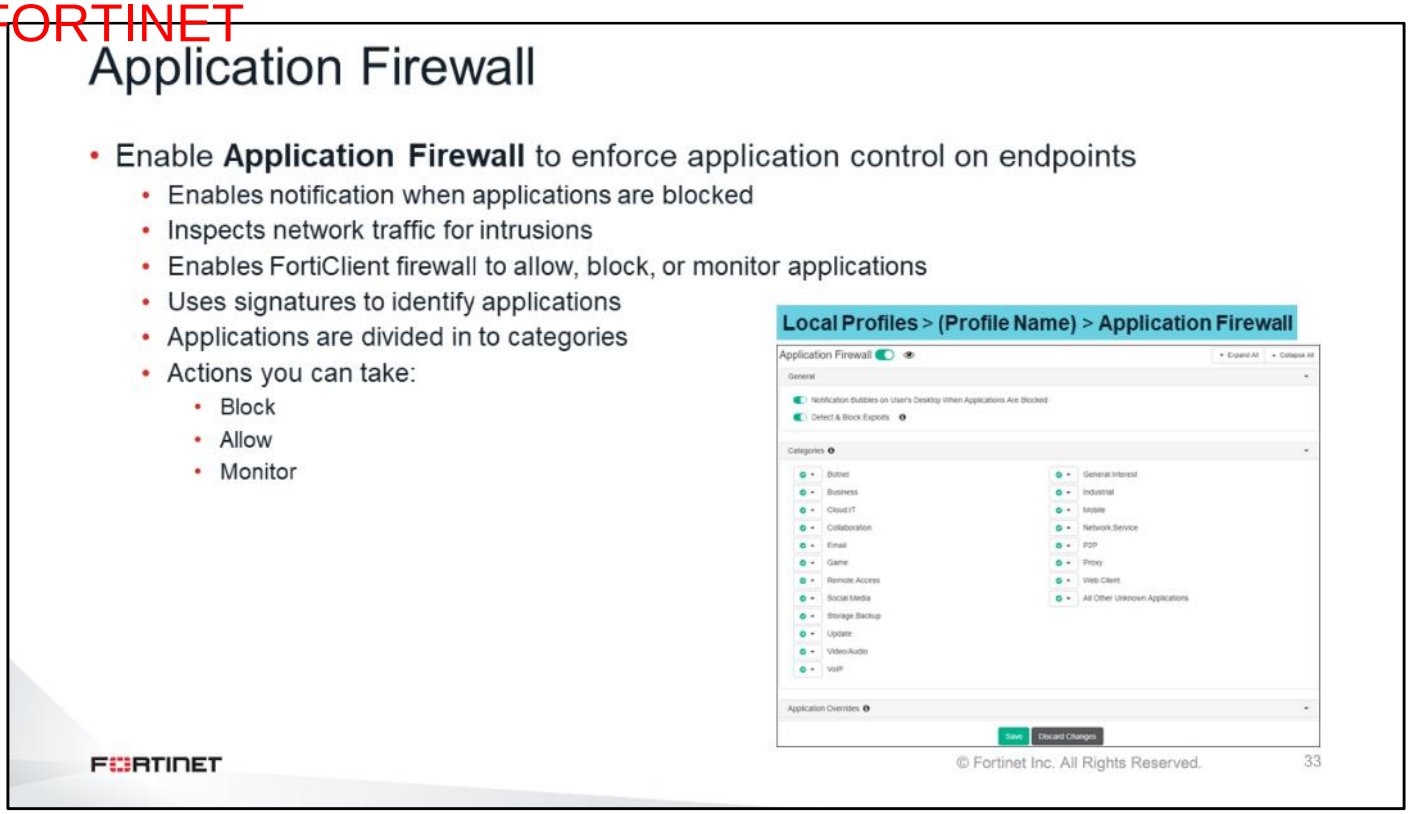
Site Categories option enables site categories from FortiGuard. When site categories are disabled, FortiClient is protected by the exclusion list. For all categories below, you can configure an action for the entire site category by selecting either **Block**, **Warn**, **Allow**, or **Monitor**. Each site category is shown in this slide image.



In **Rate IP Addresses**, you can filter URLs and resolved IP addresses at the same time and select the action for rating errors.

Note that if you enable the **Allow websites when rating error occurs** option, FortiClient will block all URLs, including the captive portal authentication page. This will prevent users from getting access to the authentication page.

The **Exclusion List** option allows you to select an action, and enter specific URLs and their type, such as simple, wildcard, or regular expression.

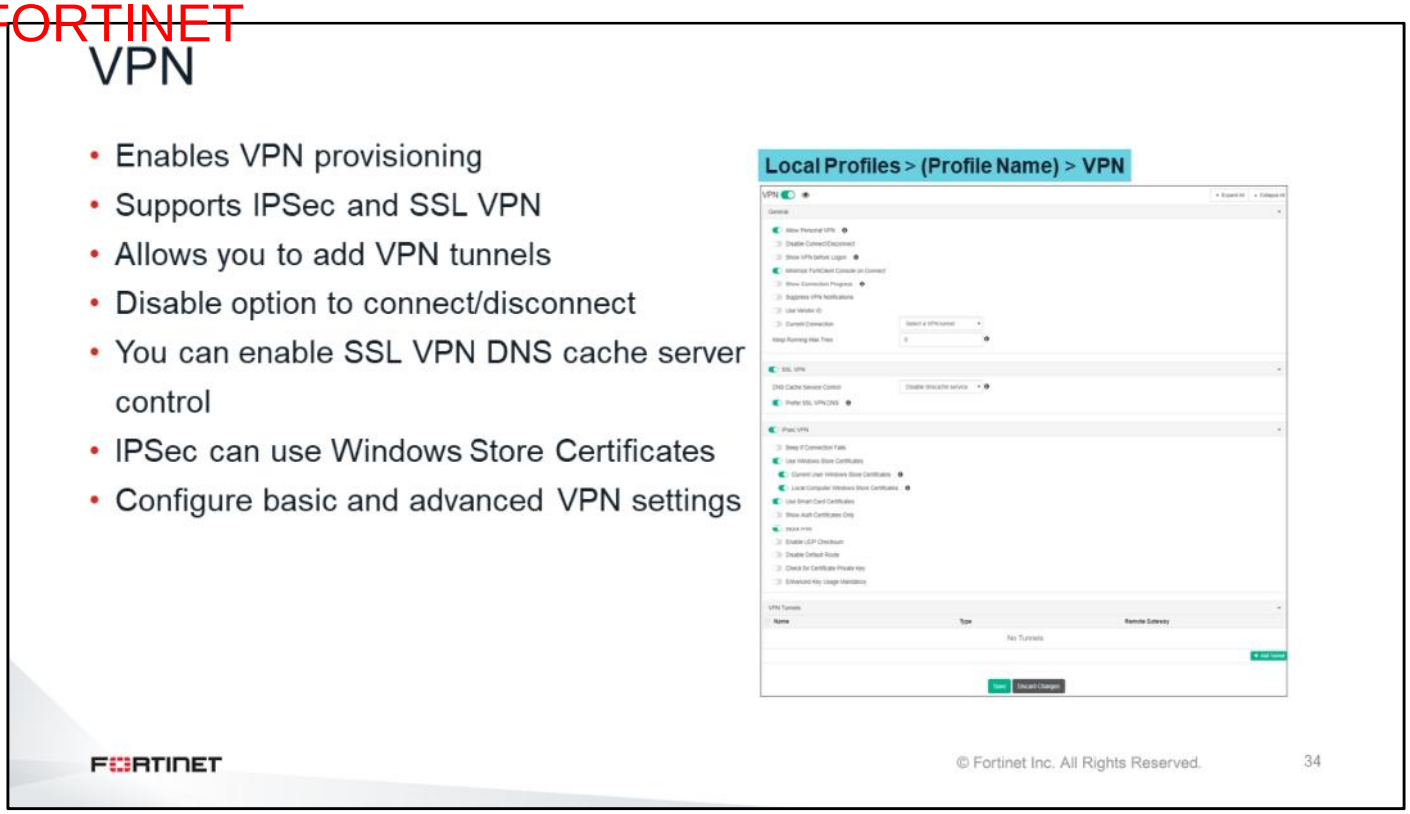


Application Firewall tab enables or disables application control.

In the **General** section, you can enable bubble notifications for blocked applications. You can also enable the inspection of network traffic for intrusions attempting to exploit known vulnerabilities.

In the **Categories** section, you can select the following actions on the categories shown in this slide image:
- Block
- Allow
- Monitor

The **Application Overrides** option allows FortiClient firewall to allow, block, or monitor applications based on their signatures. You can delete an application and add a signature to an application.

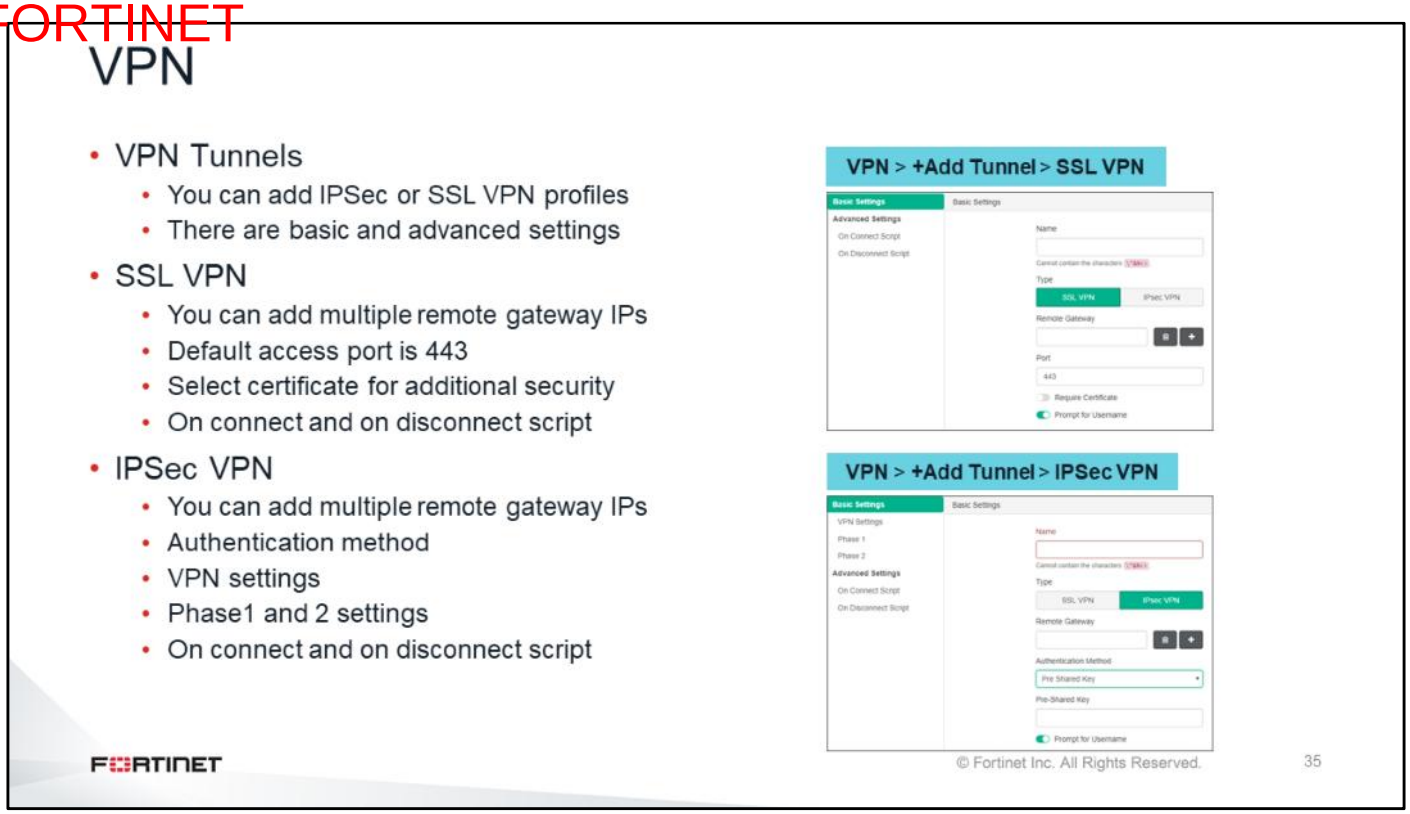


The **VPN** tab enable or disable VPN use on endpoints. There are general and specific VPN type settings available to configure.

General section allows you to enable or disable various VPN related settings. You can also select a maximum number of attempts. These options are applied to both SSL and IPSec VPN.

SSL VPN includes **DNS Cache Service Control** setting. You can select to disable, leave unchanged, or restart the DNS cache control service. You can also override the DNS server to SSL VPN DNS IP.

You can also enable or disable different IPSec VPN options that are shown in this slide image.



You can add VPN profiles for both SSL and IPsec.

The SSL VPN settings includes remote gateway IP, SSL port number, and options to request the certificate and prompt for the user name. There is also an option to enter connect and disconnect scripts, which needs to be enabled on FortiGate.

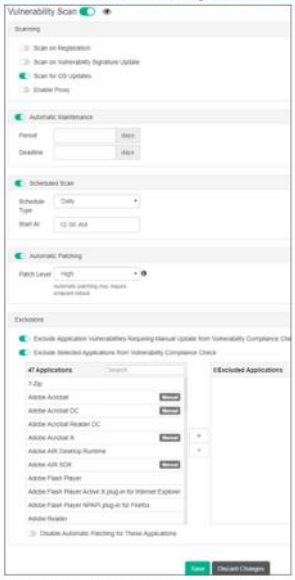
The IPSec VPN settings includes remote gateway IP, authentication method, pre-shared key (if *Pre-Shared Key* is selected for **Authentication Method**), and prompt username. You can select the IPsec mode (Main or Aggressive), options such as Mode Config, Manual Set, or DHCP over IPSec, DNS server, and so on in the **VPN Settings** pane.

You can also configure phase 1 and phase 2 settings. You can select the encryption and authentication algorithms used to generate keys for protecting negotiations and add encryption and authentication algorithms as required, and algorithms that will be proposed to the remote VPN peer. You need to select a minimum of one and a maximum of two combinations. The remote peer or client must be configured to use at least one of the proposals that you define.

Vulnerability Scan

- **Vulnerability Scan** tab enables scanning on endpoints
  - Scanning on connecting to FortiGate
  - Scan for OS and vulnerability signature updates
  - Configure automatic maintenance
  - Configure scheduled scans
  - Configure automatic patching
  - Create exclusion list

Local Profiles > (Profile Name) > Vulnerability Scan



FORTINET

 36

You can select vulnerability scan for endpoints upon connecting to a FortiGate, updating a vulnerability signature, and for OS updates.

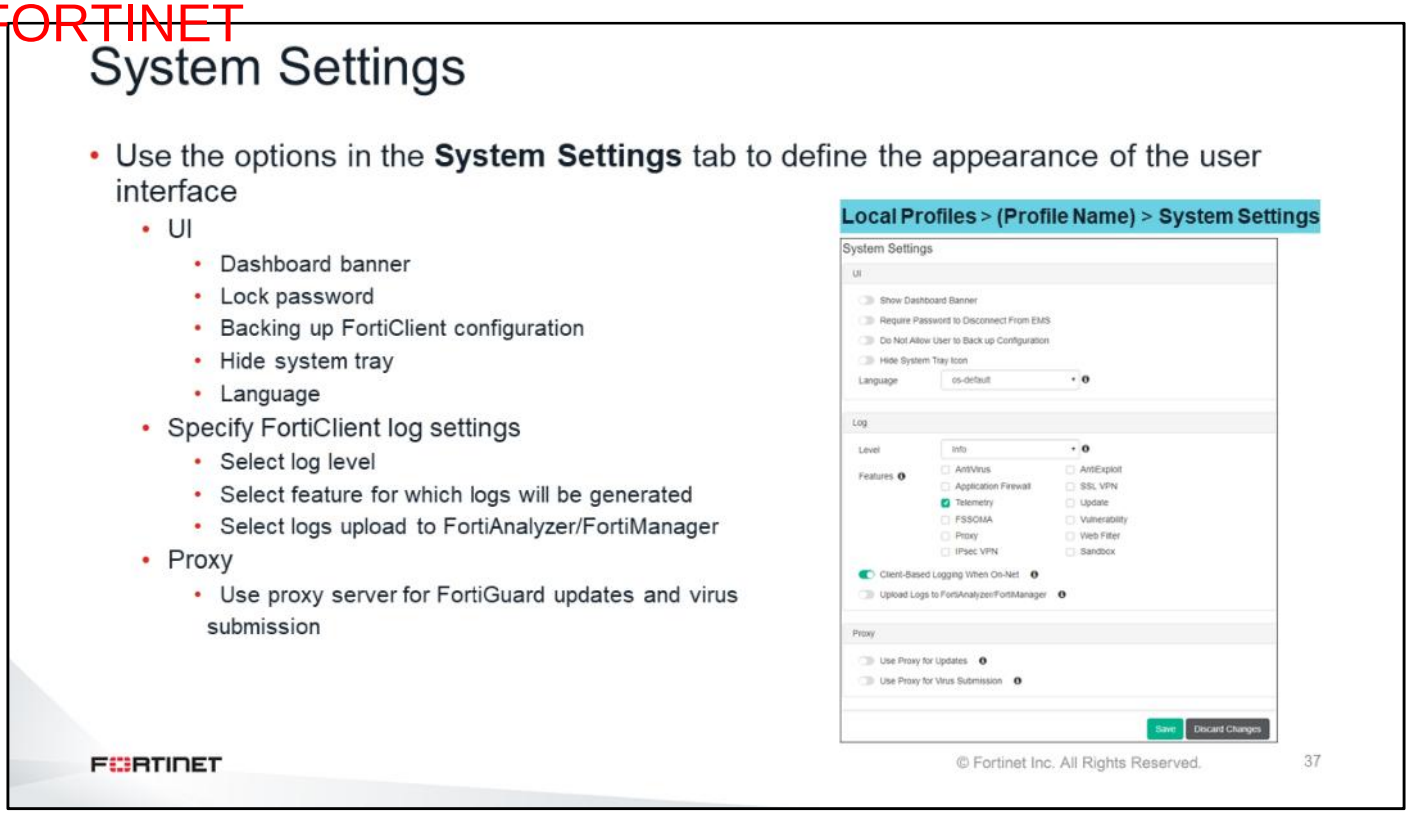
You can also select **Enable Proxy** setting to enable proxy.

Automatic Maintenance setting allows you to configure the vulnerability scan to run as part of Windows automatic maintenance. Adding FortiClient vulnerability scans to the Windows automatic maintenance queue allows the system to choose an appropriate time for the scan.

You can also schedule scans. In the **Schedule Type** drop-down list, you can select `Daily`, `Weekly`, or `Monthly`. In the **Scan On** field, you can configure the day the scan will run. This setting applies if the schedule is Monthly. You can also specify the time the scan will start.

Automatic Patching allows patches to installed automatically when vulnerabilities are detected. You can select patch severity level such as `Critical`, `High`, `Medium`, `Low` or `All`.

Exclusions allows you to exclude applications, the option are shown in this slide image. These options do not exclude applications from vulnerability scanning.



The majority of these configuration options are available for only Windows, macOS, and Linux profiles. Options such as **Upload Logs to FortiAnalyzer/FortiManager** are available for all endpoints. Some options are available only when you enable the **Advanced** view.

UI section specifies how the FortiClient user interface appears when installed on endpoints.

The **Log** section specifies log settings such as **Level** and **Features** for which logs will generate. There are different log levels available for FortiClient. This include `Info`, `Emergency`, `Alert`, `Critical`, `Notice`, `Debug`, and so on.

You can also select **Client-Based Logging When On-Net**, this includes local log messages when client is on-net and **Upload Logs to FortiAnalyzer/FortiManager**. This will require the IP address of the FortiAnalyzer/FortiManager and other settings such as upload schedule, log generation timeout, and log retention policy in days. You can also select to upload event logs from FortiClient endpoints.

The **Proxy** section allows you to enable access to FortiGuard servers and submit virus to FortiGuard using the configured proxy. You can select proxy type, IP, port, username, and password.

System Settings (Contd)

- **Update**
  - Specify whether FortiManager or Micro-FortiGuard server updates FCT
  - Enables FortiClient software update
  - Select update action, scheduling, and server location
- **FortiProxy**
  - You must enable **FortiProxy** to use the web filter options as well as some antivirus options
  - Enables **HTTPS Proxy** to inspects https traffic
  - Email server and client comforting
- **Endpoint Control**
  - Specify settings for endpoints
  - You can enable
    - **Show Bubble Notifications**
    - **Silent registration**
    - **On-Net Subnets**

Local Profiles > (Profile Name) > System Settings

FORTINET

38

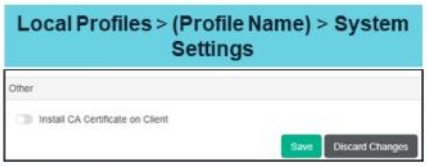
In update section, you can specify whether FortiManager or Micro-FortiGuard Server is used for FortiClient updates. You can also select FortiClient software updates, the update schedule, and FortiGuard server location.

You must enable FortiProxy to use the web filter options as well as some antivirus options. You can enable **HTTPS Proxy**. If disabled, FortiProxy no longer inspects HTTPS traffic. It also enables other useful options that are shown in this slide image.

The **Endpoint Control** section specifies the settings for endpoint. You can refer to this slide image for all the options available.

System Settings and XML

- Other
  - Enable to select and install a CA certificate on endpoints
  - Select to enable single sign-on (SSO) mobility agent
- iOS
  - Enable and browse for `.mobileconfig` file to distribute the configuration profile
- Privacy
  - Send usage statistics to Fortinet to improve product
- XML Configuration
  - Use XML editor to configure FortiClient settings

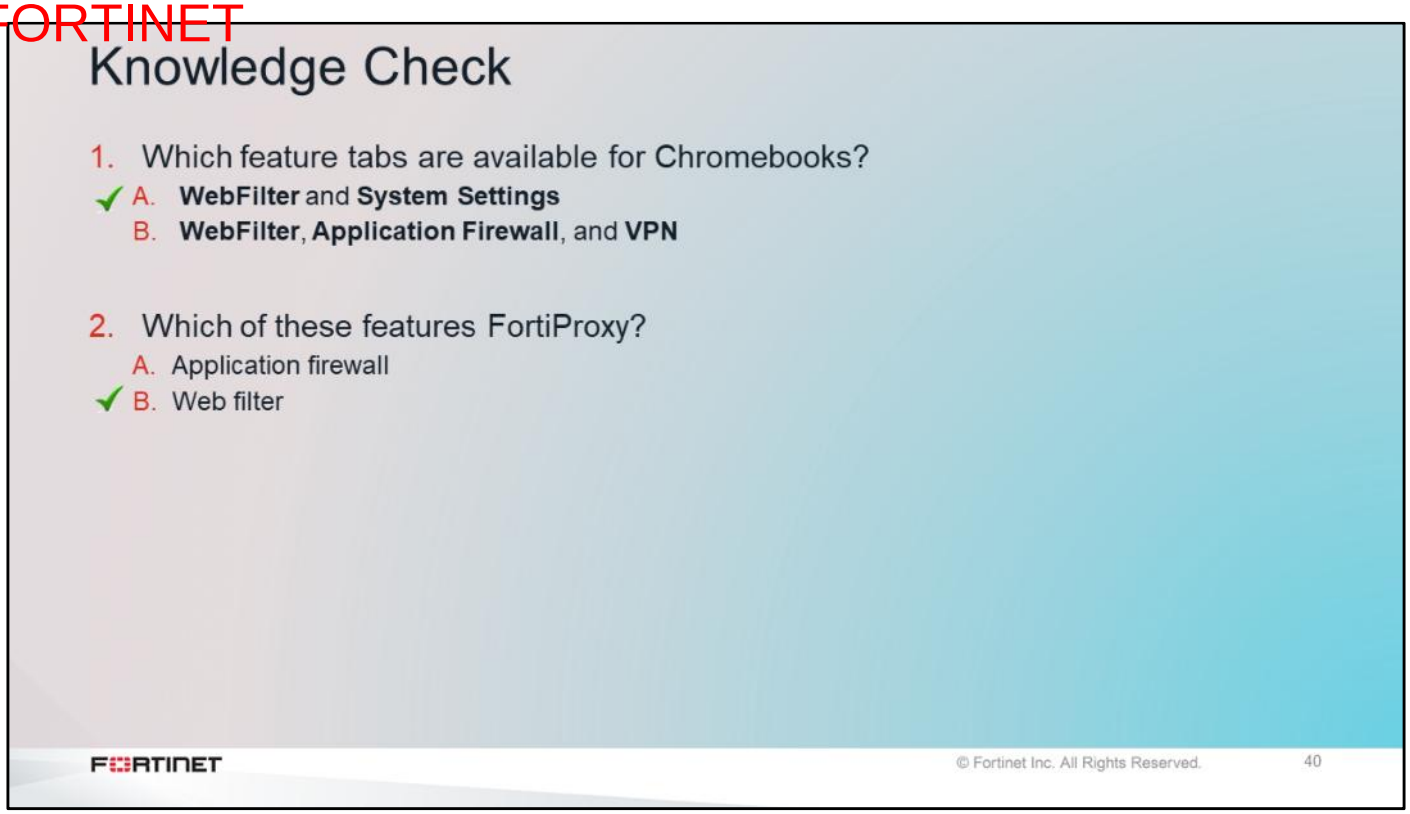


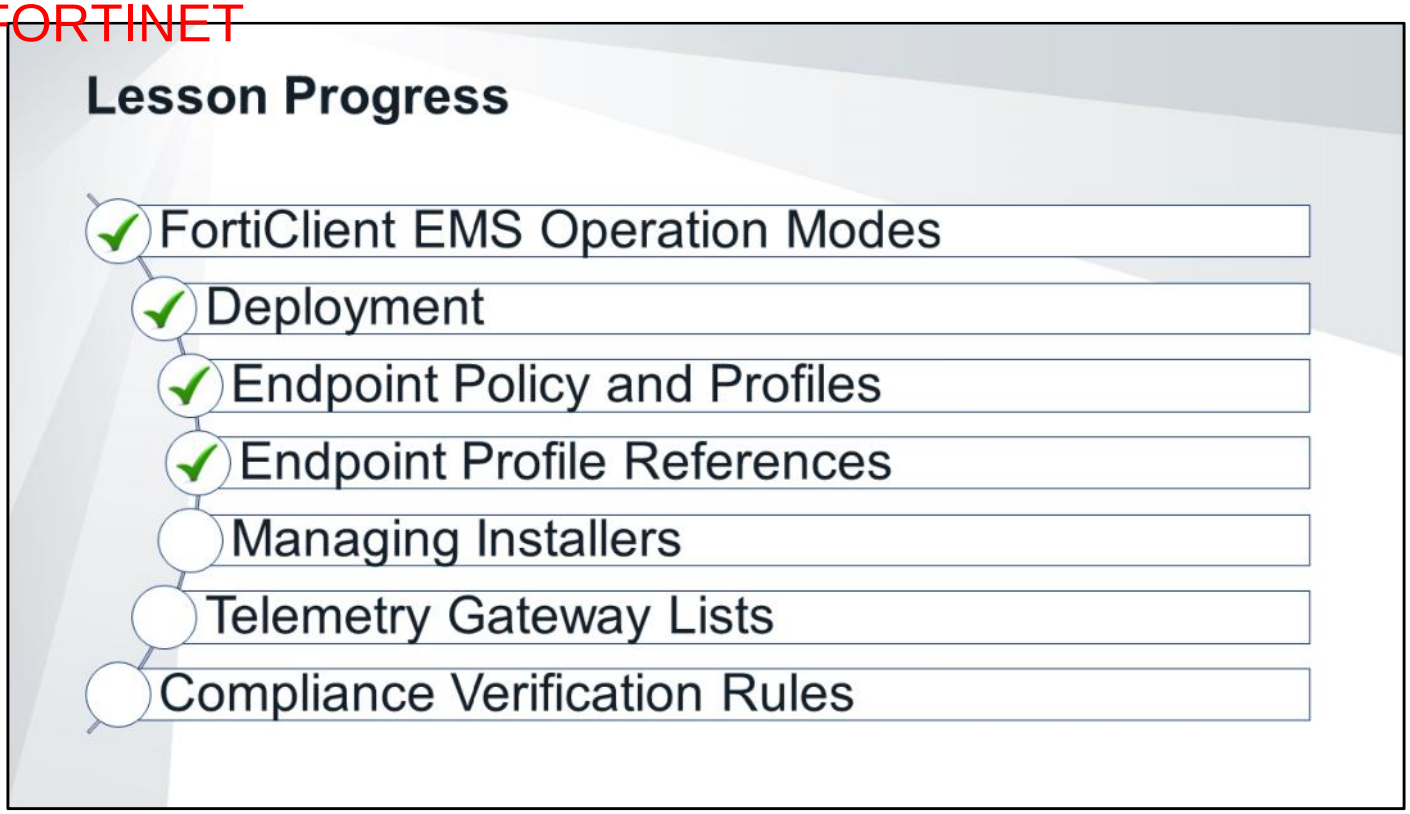
FORTINET © Fortinet Inc. All Rights Reserved. 39

The **Other** section enables CA certificate installation on the client. You can add certificates on the **Manage CA Certificates** pane. It also enables SSO mobility Agent for FortiAuthenticator. To use this feature, you need to apply a FortiClient SSO mobility agent license to your FortiAuthenticator device.

The **iOS** option allows you to upload `.mobileconfig` file to distribute the configuration profile.

In **XML Configuration** tab you can configure FortiClient options and settings in XML format.





Good job! You now understand how to use endpoint profile references.

Now, you will learn about managing installer and profile components.

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in working with deployment packages, installers, and profile components, you will be able to create deployment packages, installers, and manage CA certificates on EMS.

Deployment Packages

- Use to deploy FortiClient to endpoints
- Deployment packages include:
  - FortiClient installer, which determines release and patch
  - FortiClient features to be installed on the endpoints
- You can specify FortiClient features to include and then disable them later in a profile
- You can not edit the deployment package
- To add a package you can select
  - Version
  - General
  - Features
  - Advanced
  - Telemetry

FORTINET

 43

You can create deployment packages to deploy FortiClient to endpoints. Deployment packages include the FortiClient installer, which determines the FortiClient release and patch to install on the endpoint, as well as which FortiClient features are installed on the endpoint. Deployment packages can also include a Telemetry gateway list for connection to a FortiGate.

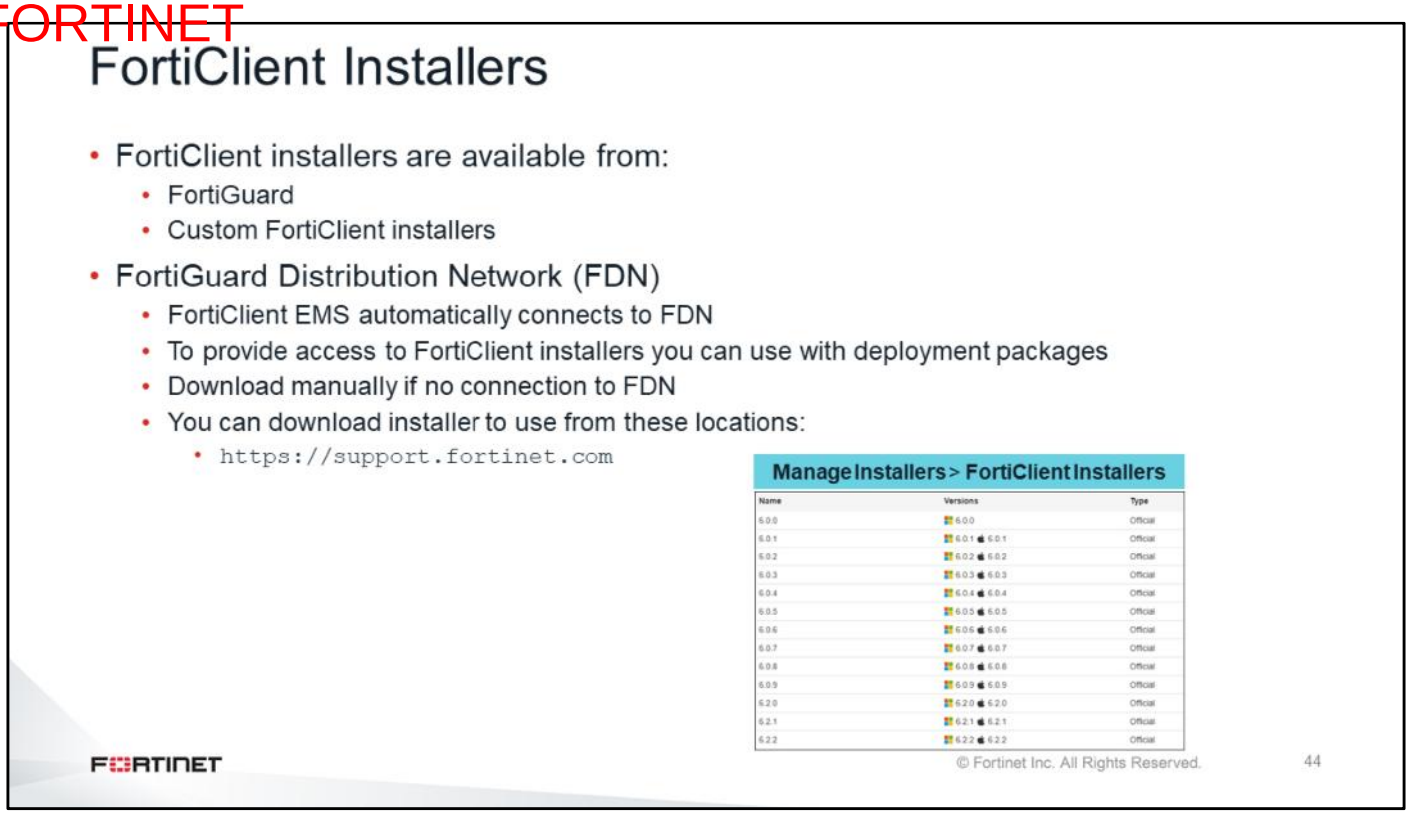
You can also specify what FortiClient features to include in the deployment package for the endpoint. You can include a feature in the deployment package, then disable the feature in the profile. Because the feature is included in the deployment package, you can update the profile later to enable the feature on the endpoint.

After you add a package to the EMS, you can not edit it. You can delete the package and edit the deployment package outside of the EMS and then can add the edited deployment package to the FortiClient EMS. When adding a package you can select an installer type, release version, patch, and enable FortiClient to automatically update to the latest release, and installer's name and notes.

In **Features** section, you can select options to enable Security Fabric Agent (enabled by default and can't be disabled); secure success (SSL and IPSec VPN); APT, and additional security features such as antivirus protection, web filtering, SSO agent, and cloud-based malware detection.

The **Advanced** section allows you to enable automatic registration, desktop shortcut, installer ID, and endpoint profile. In **Telemetry**, you can see the EMS hostname and IP address. You can also select Telemetry gateway list to connect to FortiGate (Security Fabric).

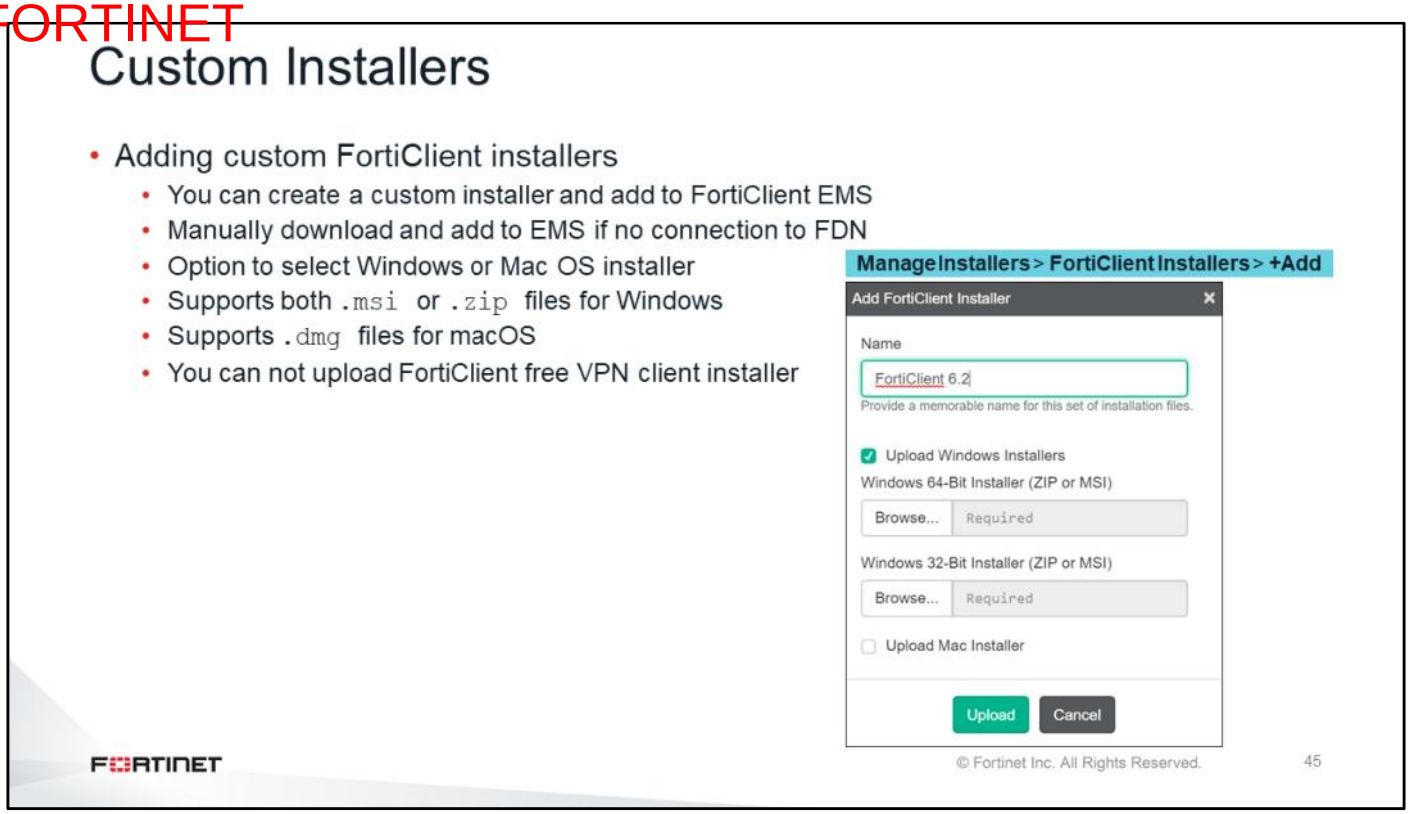
You can view the deployment packages in the **Deployment Packages** pane. You can view more details or delete packages in the Deployment Packages pane.



FortiClient EMS automatically connects to FDN to provide access to FortiClient installers that you can use with FortiClient EMS profiles. If a connection to FDN is not available, you must manually download FortiClient installers to use with FortiClient EMS.

You can download FortiClient installers to use with FortiClient EMS from `Fortinet Support site.`

After you add a FortiClient installer to FortiClient EMS, you cannot edit it. You can delete the installer from FortiClient EMS, and edit the installer outside of FortiClient EMS. You can then add the edited installer to FortiClient EMS.



You can create a custom FortiClient installer and add it to FortiClient EMS. Alternately, if a connection to FDN is not available, you may need to manually download a FortiClient installer and add it to FortiClient EMS.

There are options to select Windows or Mac installer. Windows installers must be `MSI` or `ZIP` files and macOS must be `DMG` files. You cannot upload the FortiClient free VPN client installer.

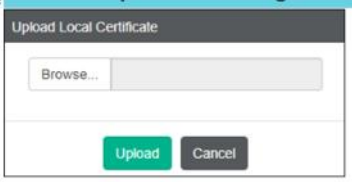
After you add FortiClient installers to FortiClient EMS, you can view them in the **FortiClient Installers** pane. By default, this page lists installers from FortiGuard first, then from uploaded installers. The following information is displayed for each installer:

- Name
- Versions
- Type

Managing CA Certificates

- You can upload or import CA certificate into FortiClient EMS
- You can upload locally by browsing to the file

Profile Components > Manage CA Certificates > Upload



- Importing certificate from FortiGate requires
  - FortiGate IP address
  - VDOM
  - Login username
  - Login password

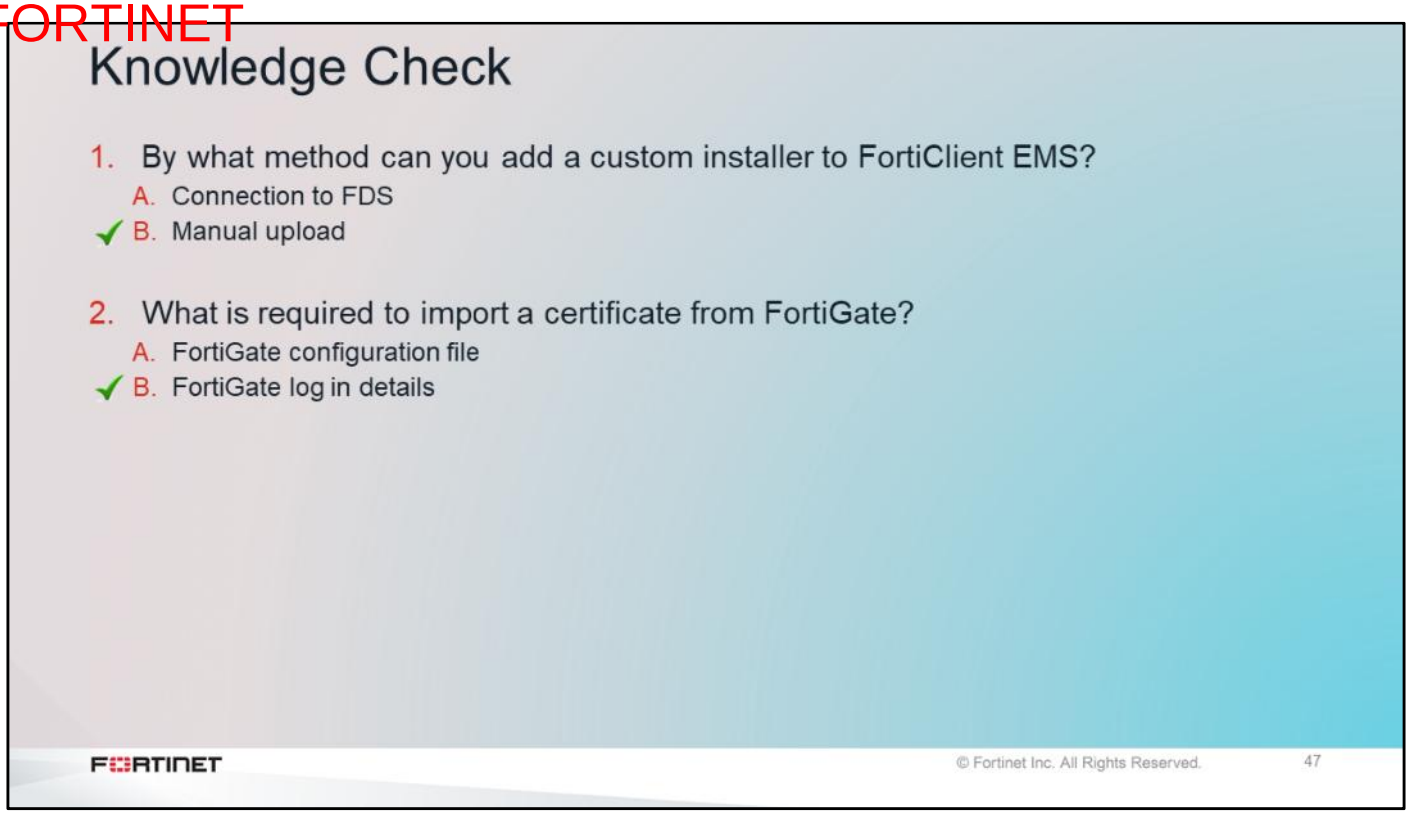
Profile Components > Manage CA Certificates > Import

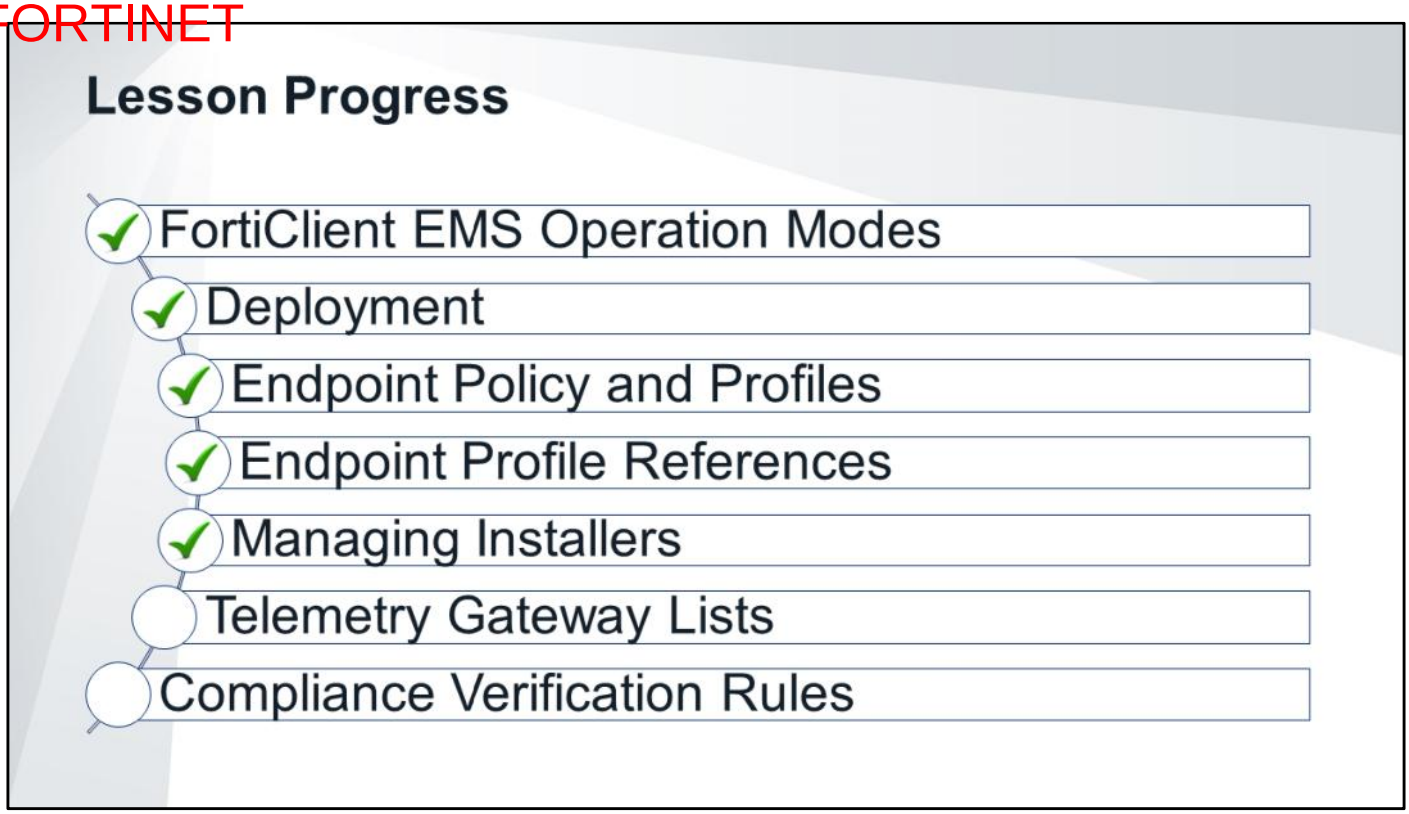
FORTINET

46

You can upload or import CA certificates into FortiClient EMS. You can upload CA certificates locally. To import a certificate from FortiGate, you need FortiGate's login details.

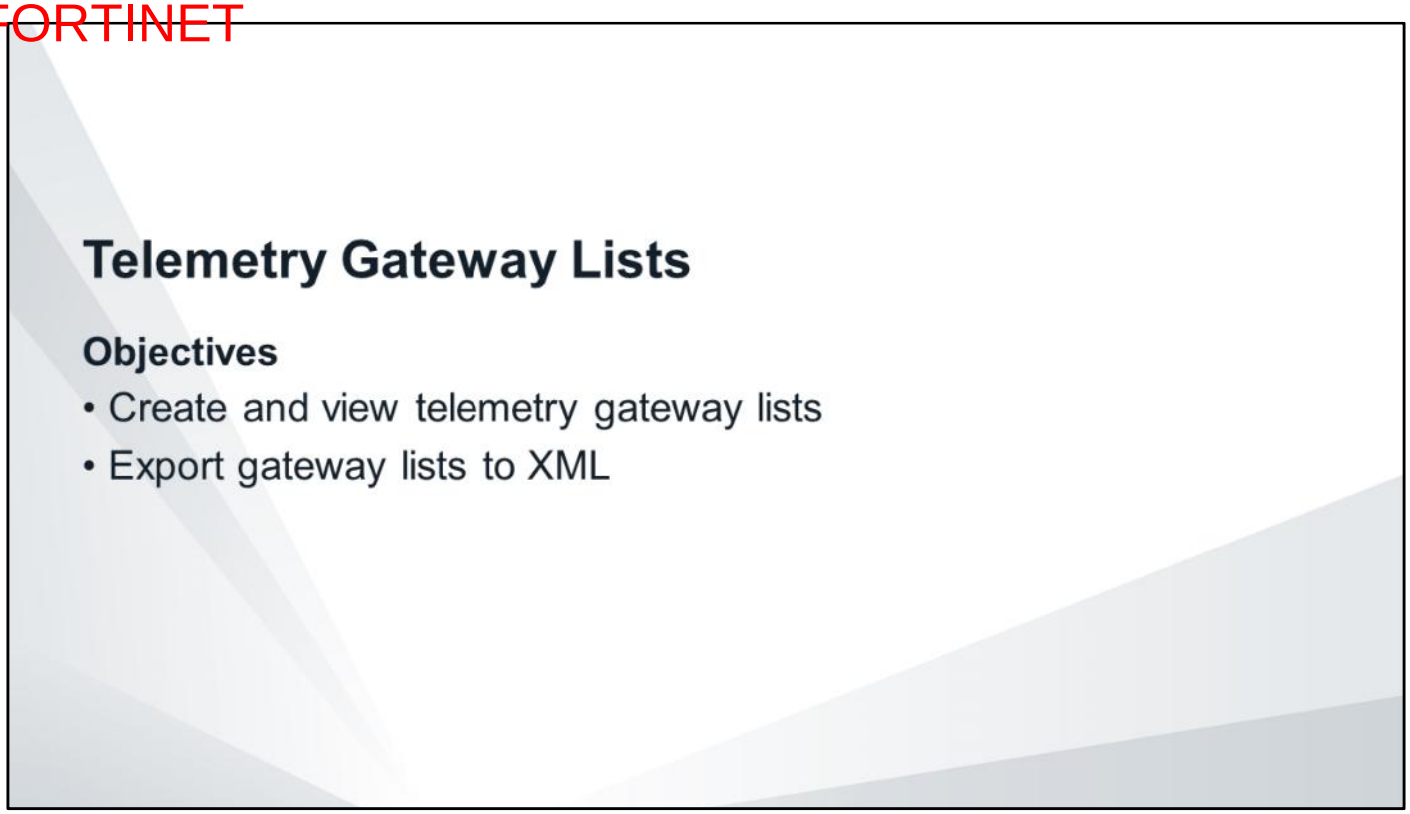
FortiClient EMS uses FortiGate's HTTPs port to import certificates.





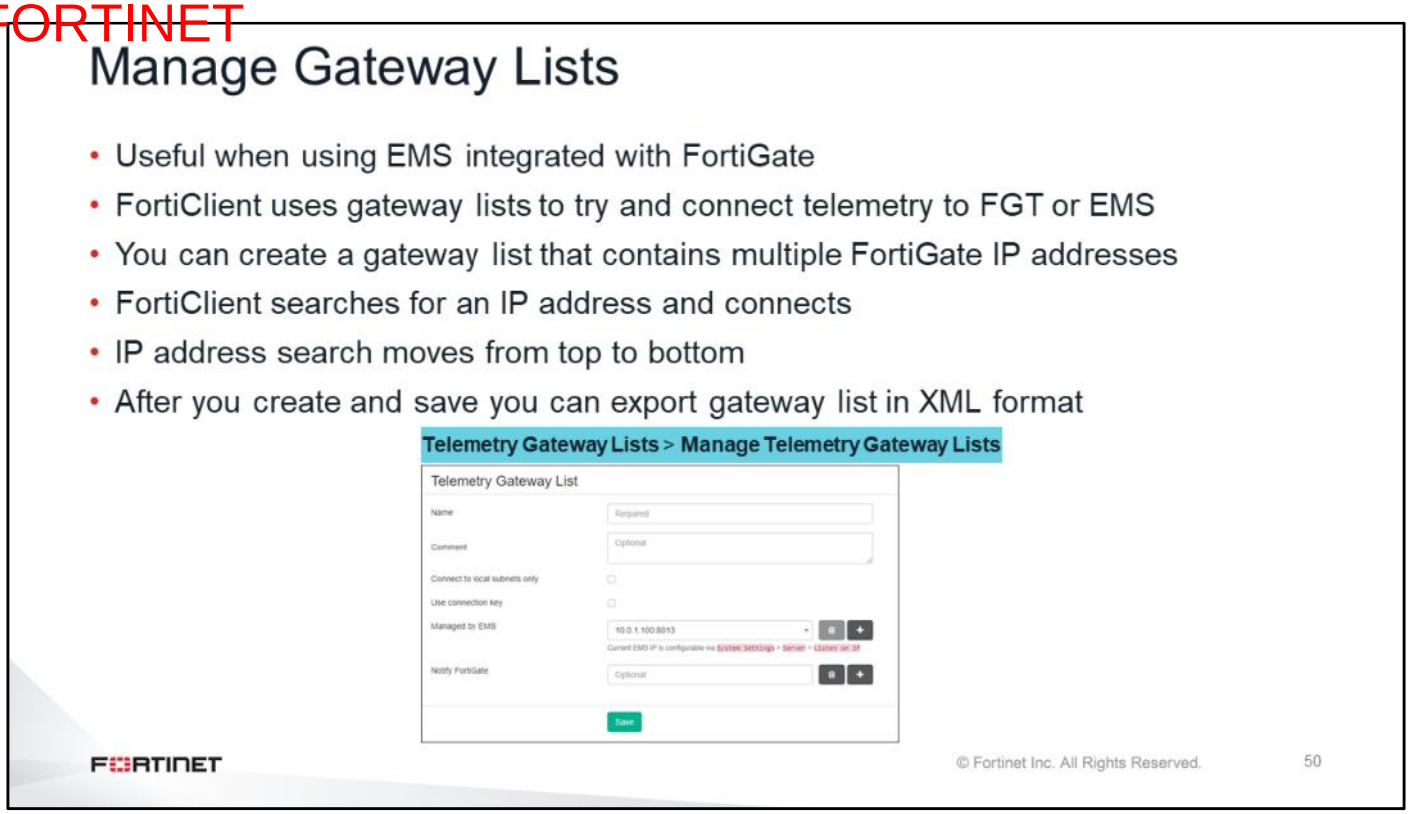
Good job! You now know how to manage deployment packages and installers.

Now, you will learn about telemetry gateway lists.



After completing this section, you should be able to achieve the objectives shown on this slide.

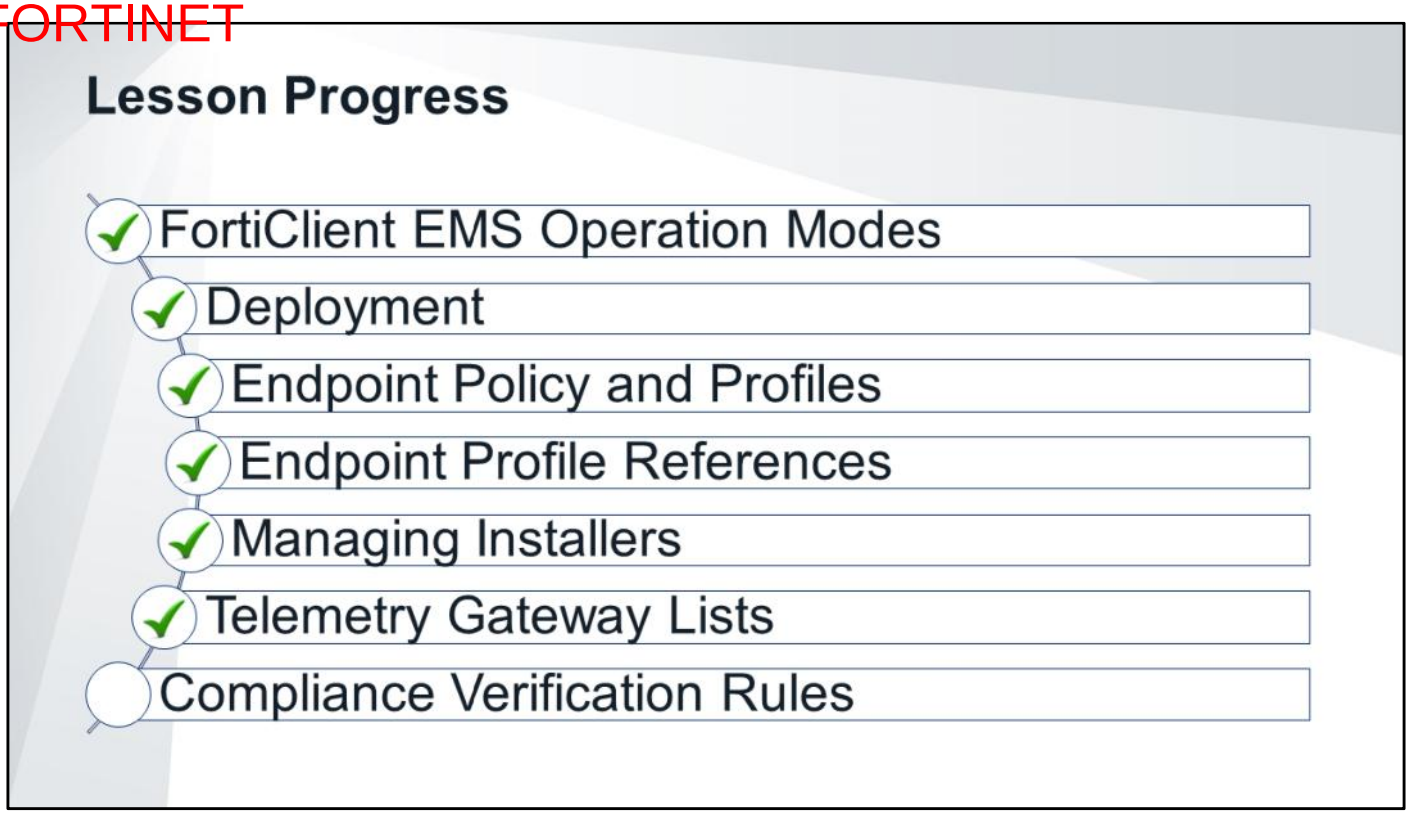
By demonstrating competence in creating, viewing, and exporting gateway lists, you will be able to work with them in your network.



Gateway lists are useful when using FortiClient EMS integrated with FortiGate. If you are using EMS only, then you're not required to use a gateway list. You can create a gateway list that contains IP addresses for multiple FortiGate devices. FortiClient searches for IP addresses in its subnet in the gateway IP list, and then connects to the FortiGate that is in the same subnet as the host system. If FortiClient cannot find any FortiGate devices in its subnet, it attempts to connect to the first reachable FortiGate in the list, starting from the top. The order of the list is maintained as it was configured in the gateway list.

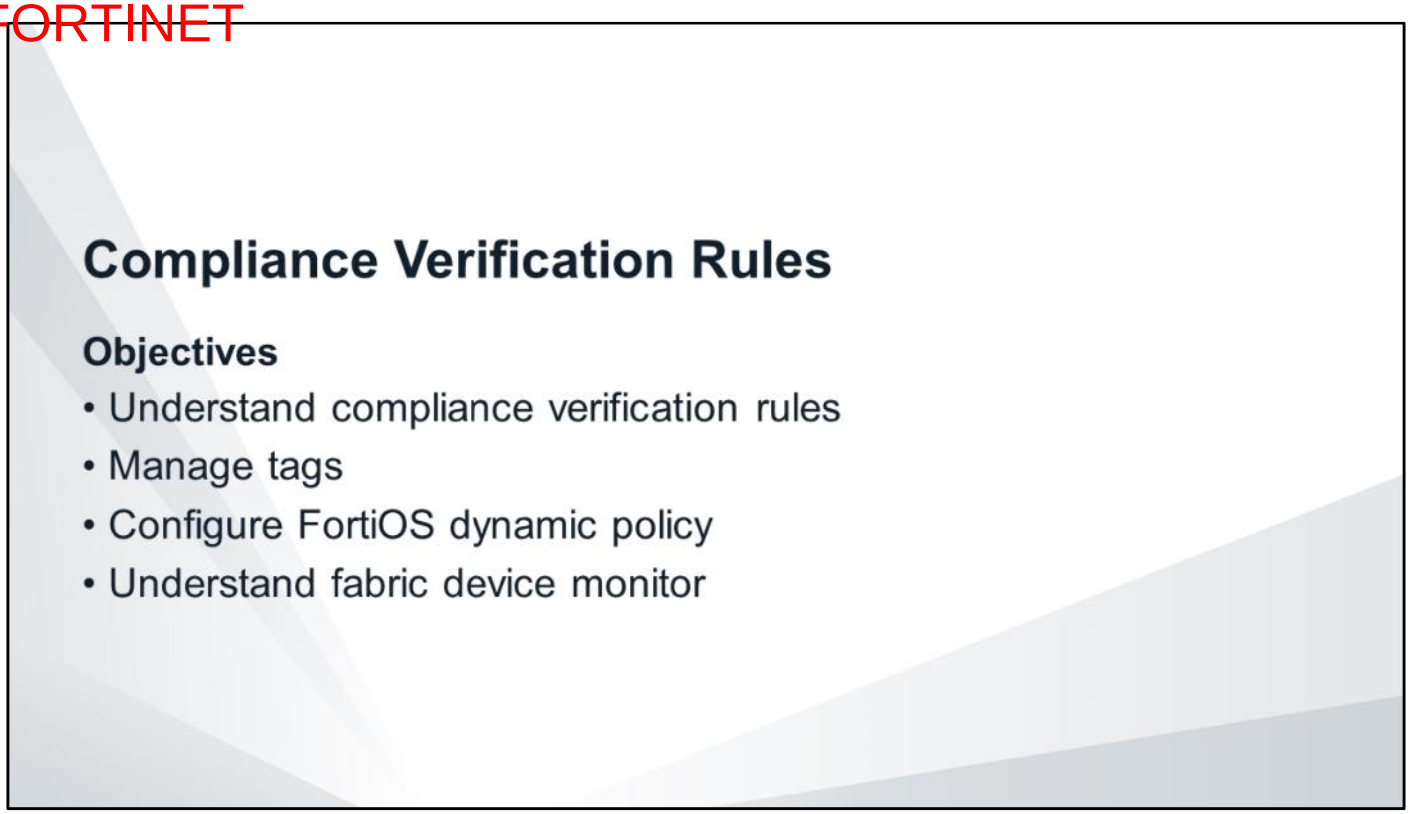
You need all the information that are shown in this slide image to create a gateway list.

After you create and save a gateway list, the **Export XML** button appears, and you can export the list to a configuration file in XML format.
You can select gateway lists in endpoint policies. When you assign the IP list, and the FortiClient Telemetry data connection process has started, the endpoint connects to a FortiGate device or EMS, based on the gateway list.



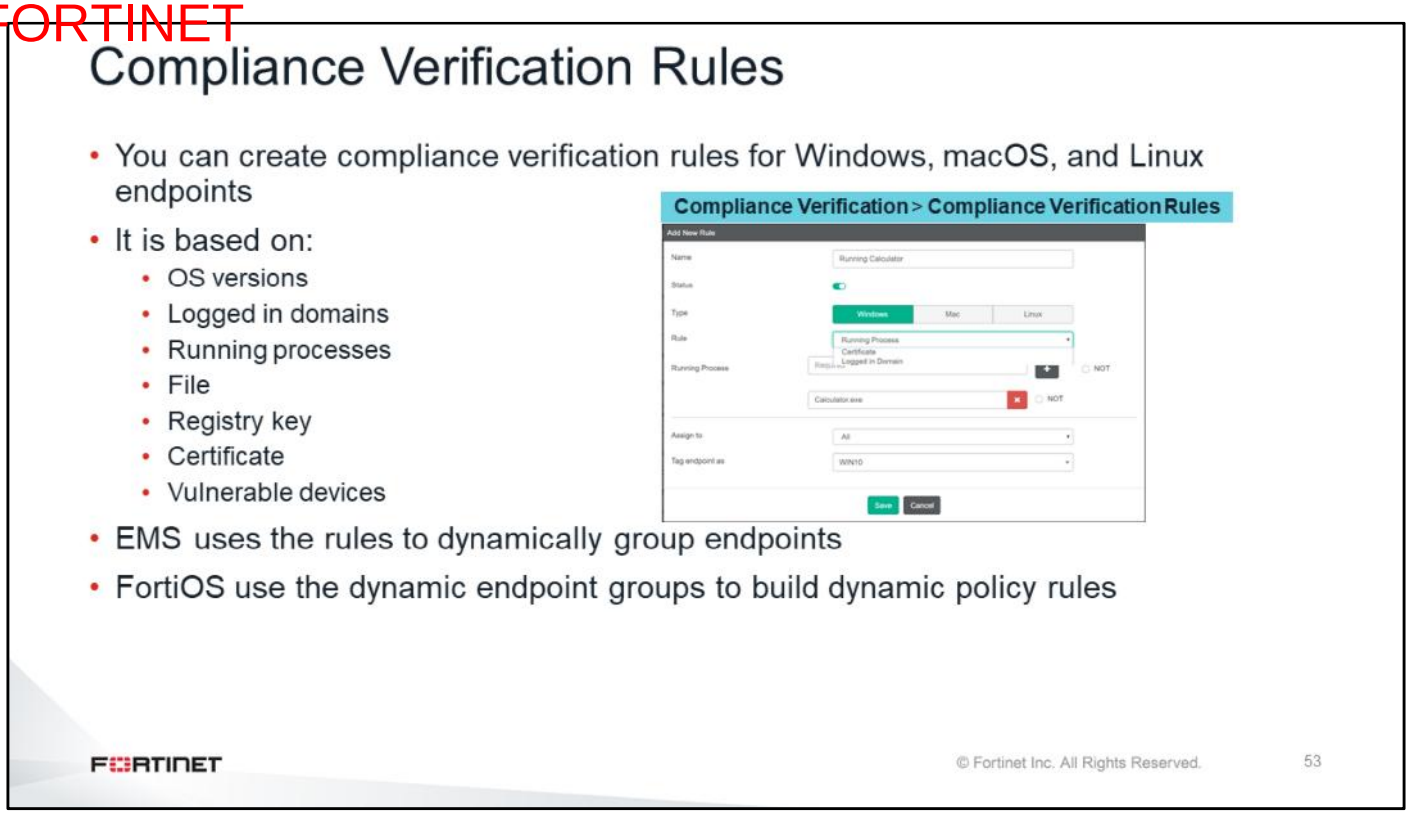
Good job! You now understand telemetry gateway lists.

Now, you will learn about compliance verification rules.



After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in compliance, tags, and FortiOS viewing, you will be able to create compliance verification rules for endpoints.

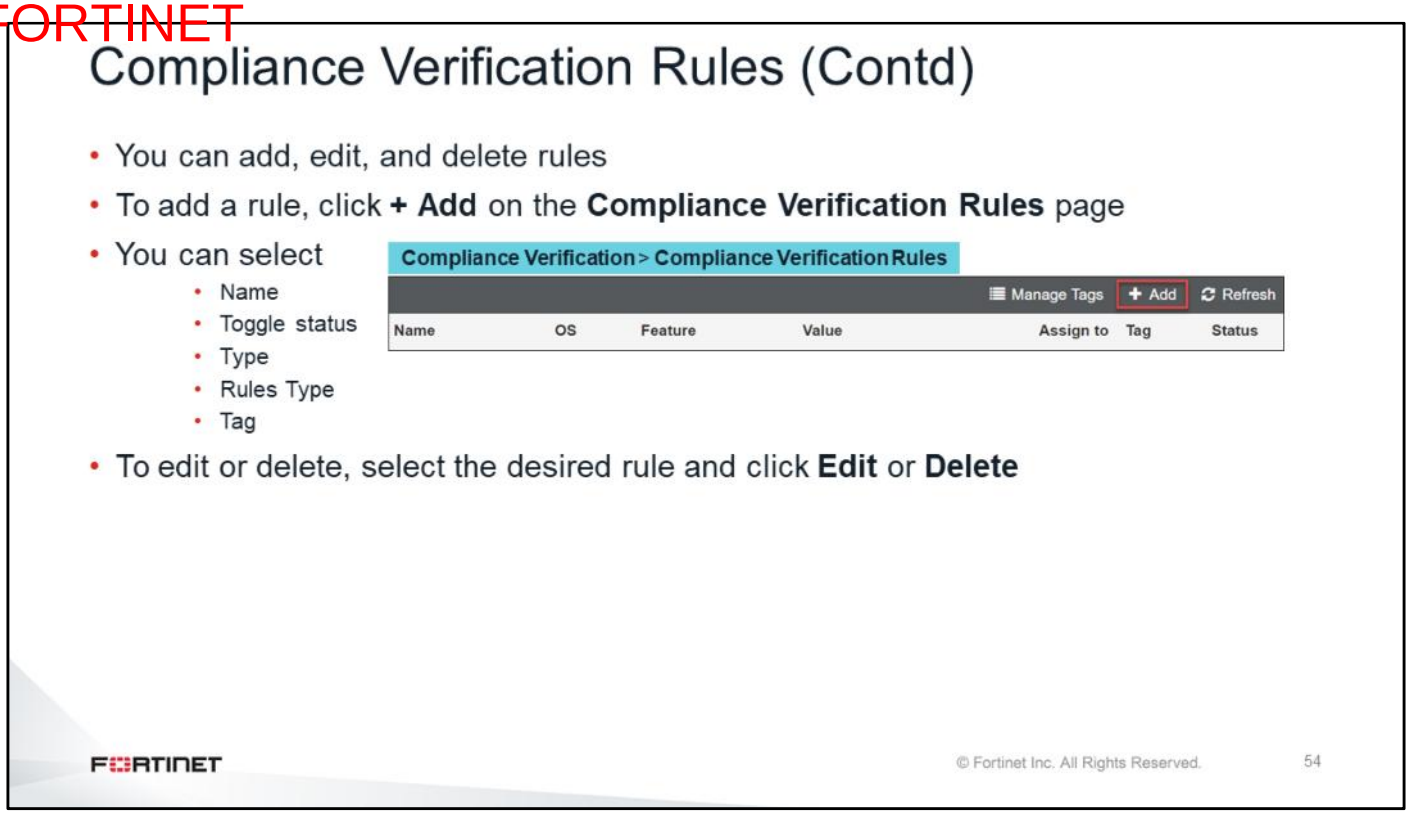


You can create compliance verification rules for Windows, macOS, and Linux endpoints based on their OS versions, logged in domains, running processes, and other criteria. EMS uses the rules to dynamically group endpoints. FortiOS 6.2.0 and later versions can use the dynamic endpoint groups to build dynamic policy rules to enforce access control based on EMS compliance rules.
The rules are based on the following:

- The **OS Versions** option allows you to select OS version. Endpoint must installed with selected OS.
- The **Logged in Domain** option allows you to add domain name. Endpoint needs to belong to that domain to satisfy the rule.
- In **Running Processes**, you can enter a process name. You can also use the NOT option to indicate that the rule requires that a certain process is not running.
- The **File** option allows you to enter a file path. You can enter multiple files and use the NOT option to satisfy the rule.
- The **Registry Key** option allows you to use the registry key value for compliance. You can use the NOT option and the endpoint must satisfy all conditions to satisfy the rule, if there are multiple values.
- In the **Certificates** option, you can enter the subject and issuer from CN fields of certificate. You can add multiple certificates and use the NOT option. The endpoint must satisfy all conditions to satisfy rule.
- The **Vulnerable Devices** option allows you to select severity level. The endpoint is considered as satisfying the rule if it has vulnerability with severity level, configured in the rule.

The following occurs when using compliance verification rules with EMS and FortiClient:

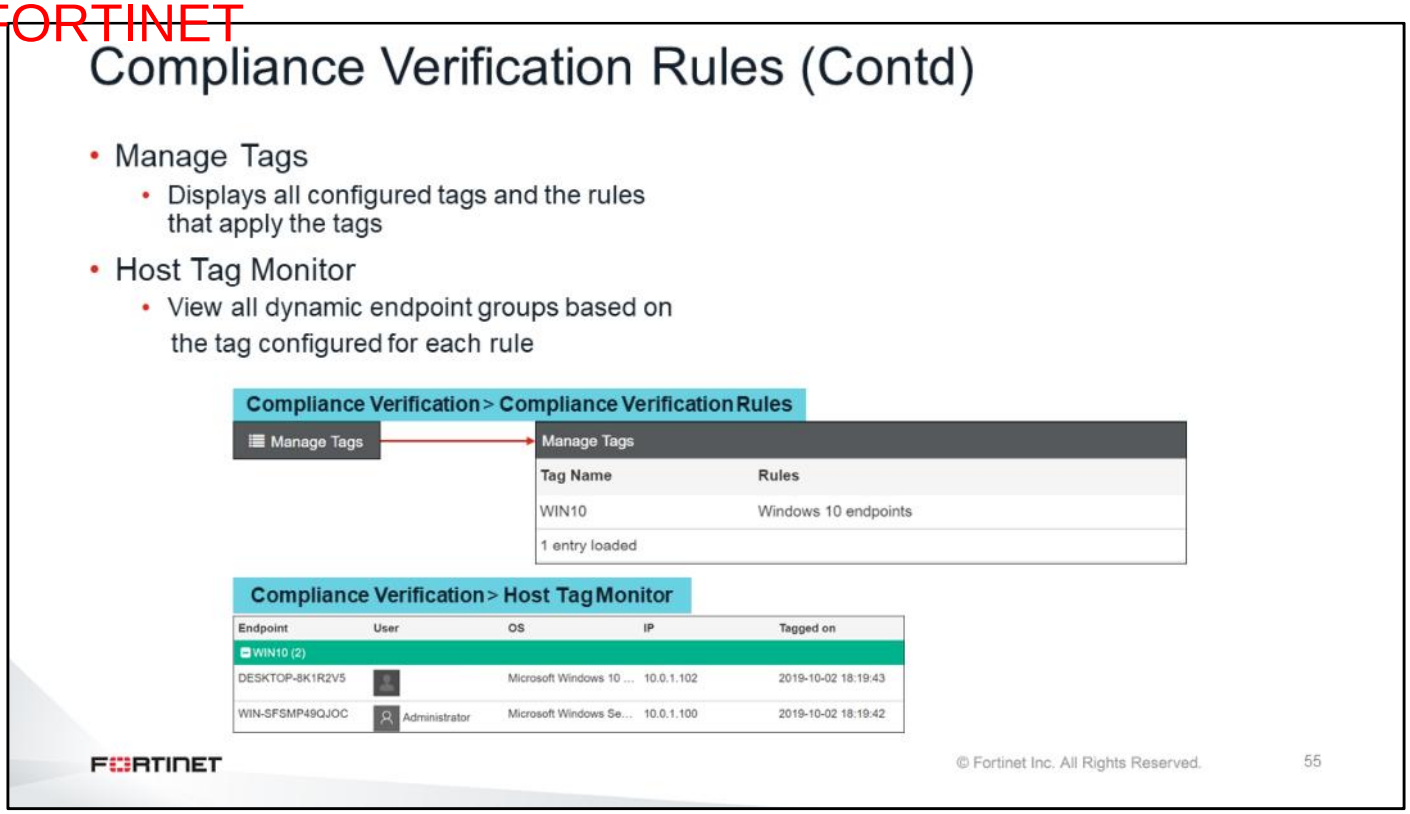
- EMS sends compliance verification rules to endpoints through Telemetry communication
- FortiClient checks endpoints using the provided rules and sends the results to EMS.
- EMS receives the results from FortiClient.
- EMS dynamically groups endpoints together using the tag configured for each rule. You can view the dynamic endpoint groups in **Compliance Verification** > **Host Tag Monitor**.



You can create, edit, and delete compliance verification rules for Windows, macOS, and Linux endpoints. You can also view and manage the tags used to dynamically group endpoints. When creating rule, you can select:

- Name
- Toggle status
- Type
- Rules Type
- Tag

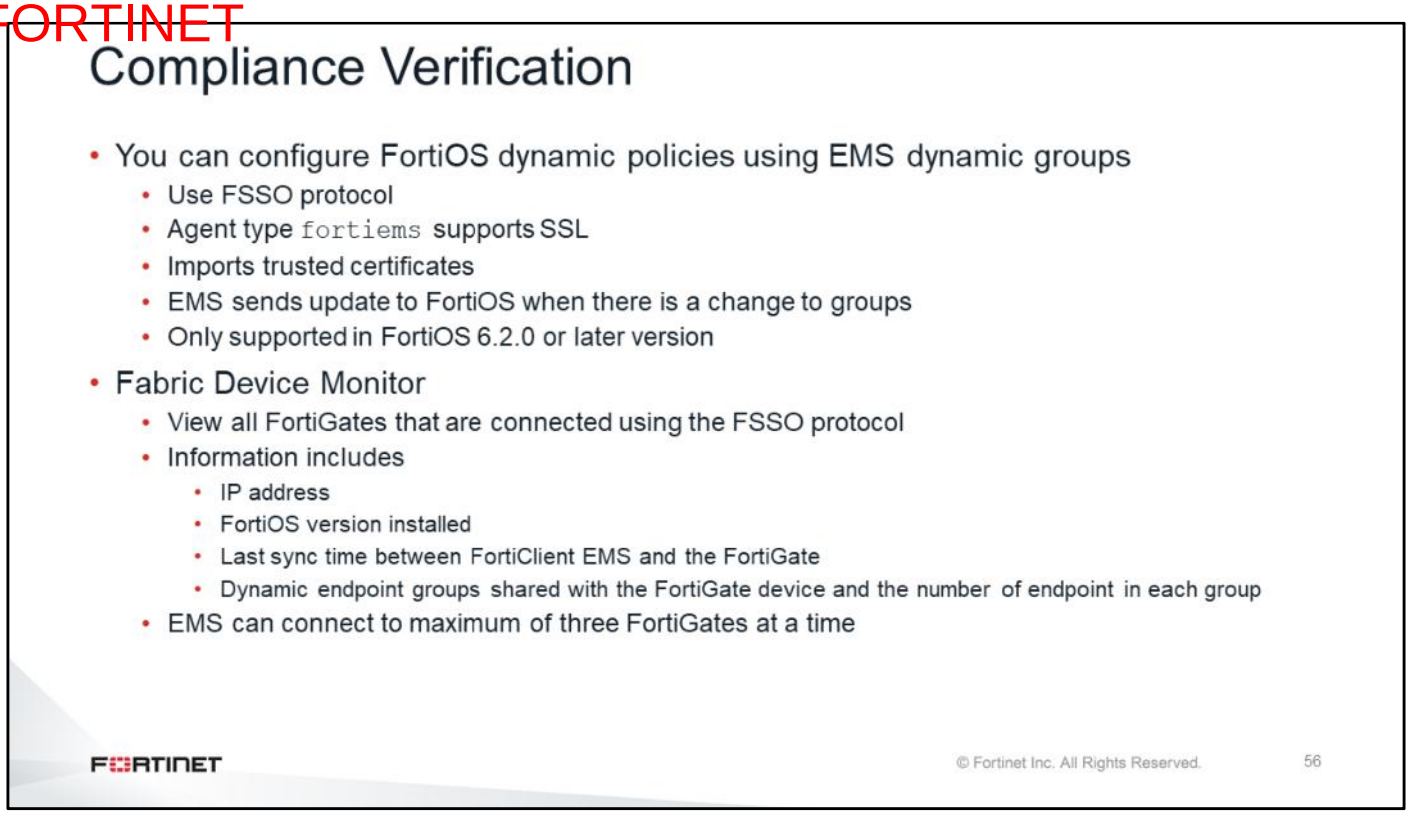
When creating rules, the value that you select in the **Type** field for Windows, Mac, or Linux can affects what rule types that are available.



The **Manage Tags** window displays all configured tags and the rules that apply to the tags to endpoints that satisfy the rule. You can delete tags that do not have any rules attached.

You can view all dynamic endpoint groups in **Host Tag Monitor**. EMS creates dynamic endpoint groups based on the tag configured for each rule.

You can also view the FortiGates that are part of the dynamic access control in **Compliance Verification** > **Fabric Device Monitor**.



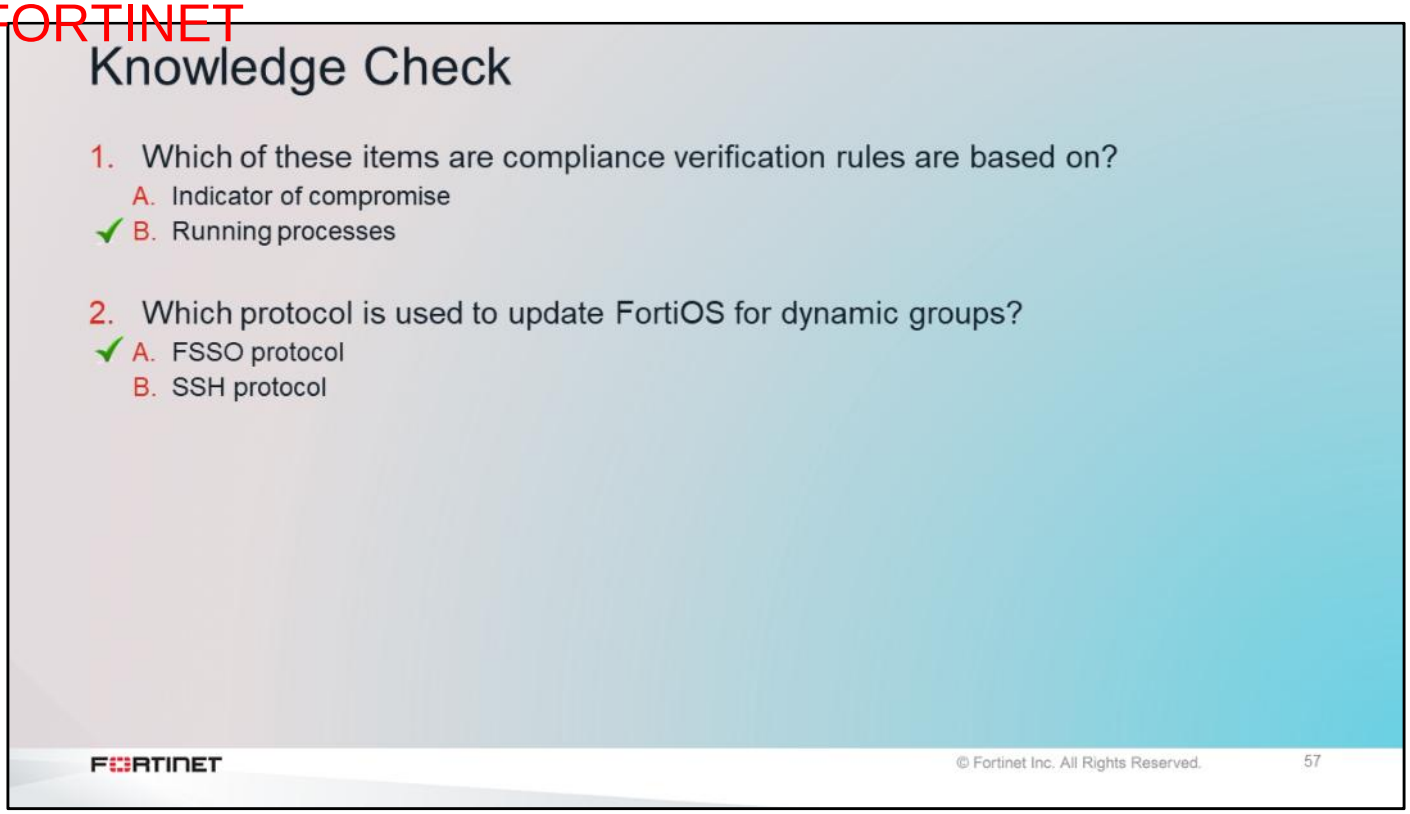
You can configure FortiOS to receive the dynamic endpoint groups from EMS through the FSSO protocol, using the new `fortiems` FSSO agent type, which supports SSL and imports trusted certificates. When a change to the dynamic endpoint groups occurs, EMS sends the update to FortiOS, and FortiOS updates its dynamic policies accordingly. This feature is only available for FortiOS version 6.2.0 or later.

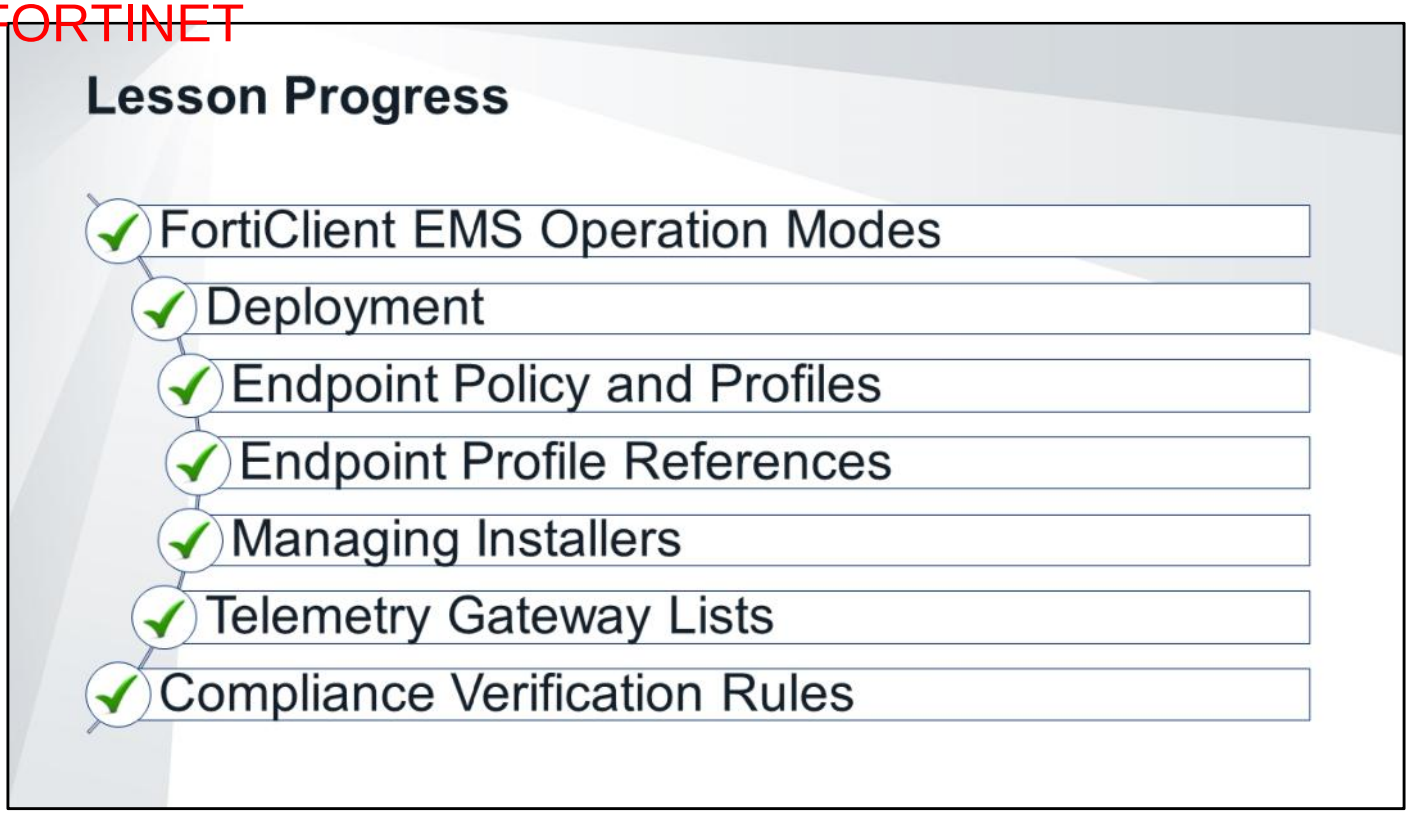
The following configuration is necessary for this feature:

1. In FortiClient EMS, create compliance verification rules.
2. After Telemetry communication has occurred between EMS and FortiClient, ensure that EMS has dynamically grouped endpoints based on the compliance verification rules.
3. In FortiOS, configure the following options to allow FortiOS to pull dynamic endpoint groups from EMS:
   - Create the fortiems FSSO agent.
   - Configure EMS FSSO groups.
   - Create a user group based on EMS dynamic endpoint group tag.
4. In FortiOS, create a dynamic firewall policy for the user group.

When a dynamic endpoint group event occurs (such as an endpoint being added to or removed from a dynamic endpoint group), EMS sends the updates to FortiOS. FortiOS updates firewall policies accordingly, providing dynamic access control based on endpoint status. EMS can be connected to a maximum of three FortiGates at a time using the FSSO protocol

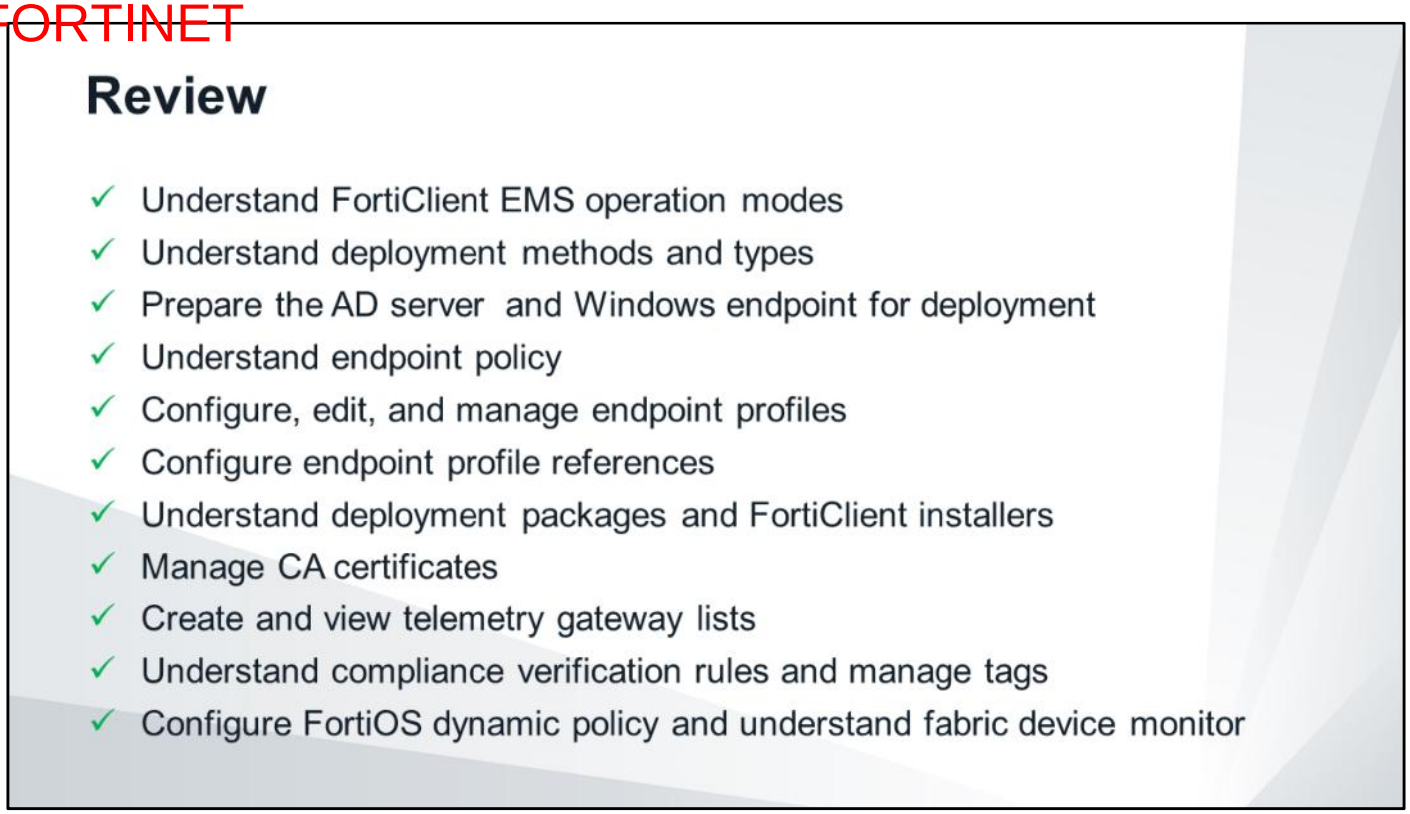
On the **Fabric Device Monitor** page, you can view all FortiGates that are connected to EMS using the FSSO protocol. EMS can be connected to a maximum of three FortiGates at a time via the FSSO protocol.





Congratulations! You have completed this lesson.

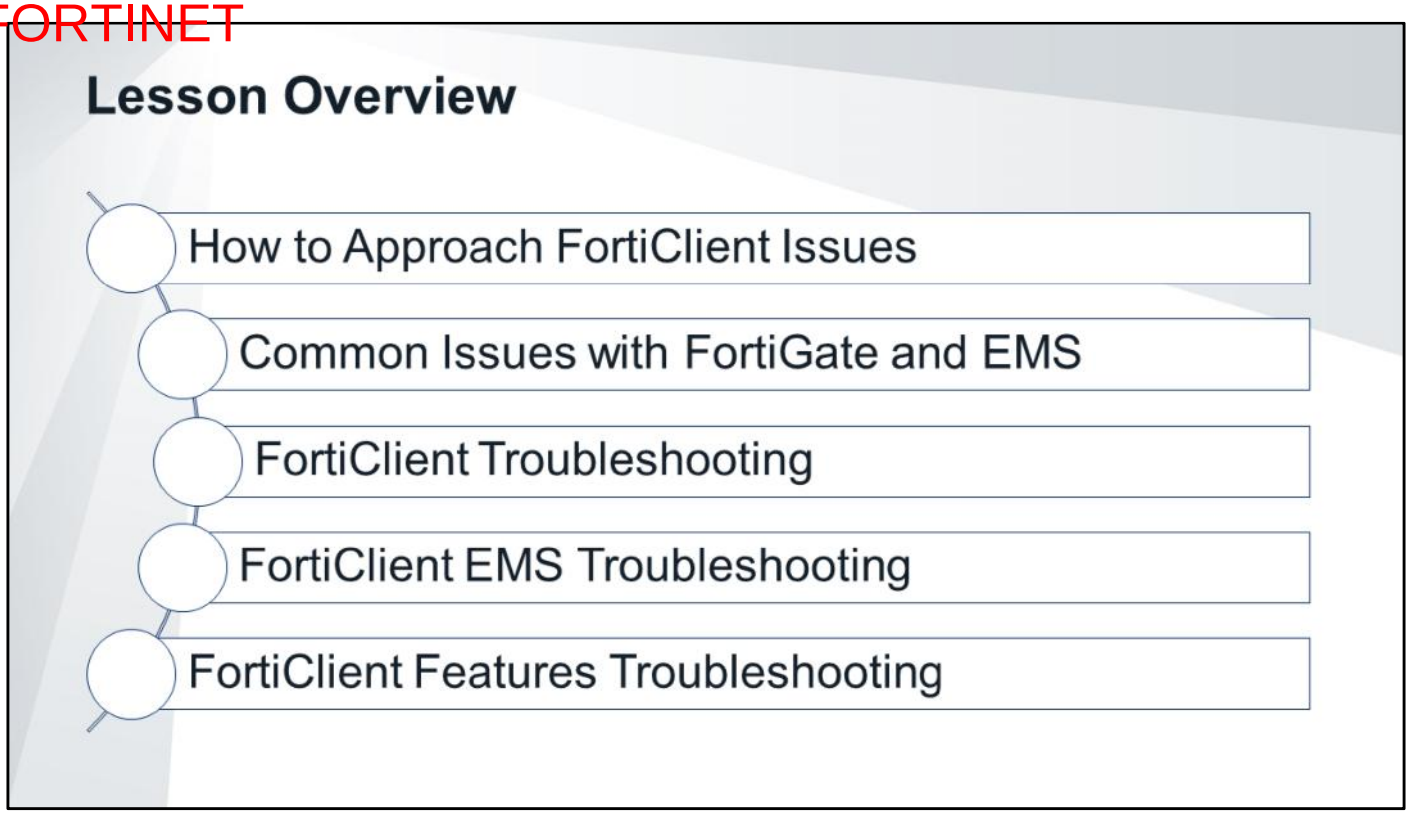
Now, you will review the objectives that you covered in this lesson.



This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to use FortiClient EMS operation modes, endpoint policy and profiles, profile references, and components. You also learned about deployment types, gateway lists, and compliance verification rules.

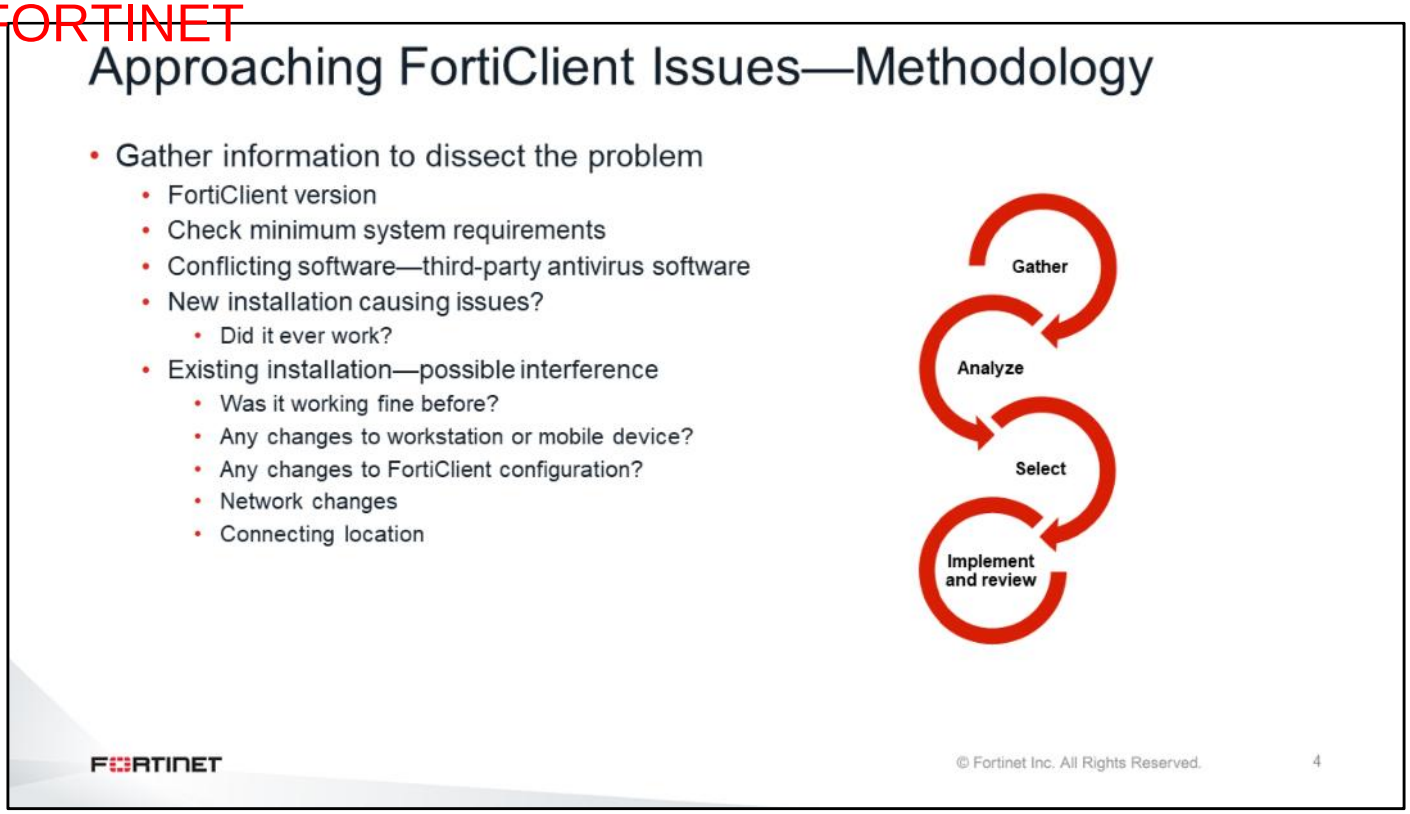
In this lesson, you will learn how to diagnose and troubleshoot FortiClient issues and FortiClient EMS issues.



In this lesson, you will learn about the topics shown on this slide.

After completing this section, you should be able to approach and troubleshoot FortiClient and FortiClient EMS issues.

By demonstrating competence in approaching and troubleshooting FortiClient issues, you will be able to solve FortiClient and FortiClient issues.



Before you can resolve a FortiClient issues, you need to identify the issue by gathering information to pinpoint and define it.

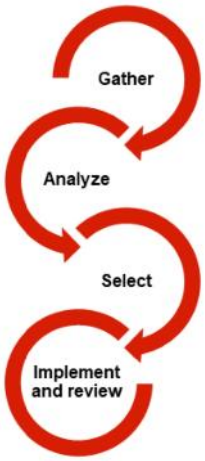
For example, if the issue is *registering FortiClient to FortiGate or FortiClient EMS*, ask and answer the following questions:
Has the registration process ever worked? Is the existing installation not working?

If the answer to these questions is yes, check for possible changes, such as changes to the device (OS updates, changes to administrator permissions), connection location (working from the office but not from home), and configuration and network changes.

Now you know the exact nature of the problem: *FortiClient is not registering from home*. The next step is to analyze the problem, which leads to possible opportunities to resolve the issue.

Approaching FortiClient Issues—Methodology (Contd)

- Analysis
  - Test on different workstation or mobile device
  - Other users having similar problems
  - Expected behaviour
    - Different behaviour
    - Reproducibility–always, random, unable to duplicate
- Possible solutions
  - List all possible options
  - Evaluate options in lab
  - Document
    - Implementation plan
    - Backup plan
- Implement and review the results
  - Monitoring and evaluation



FORTINET

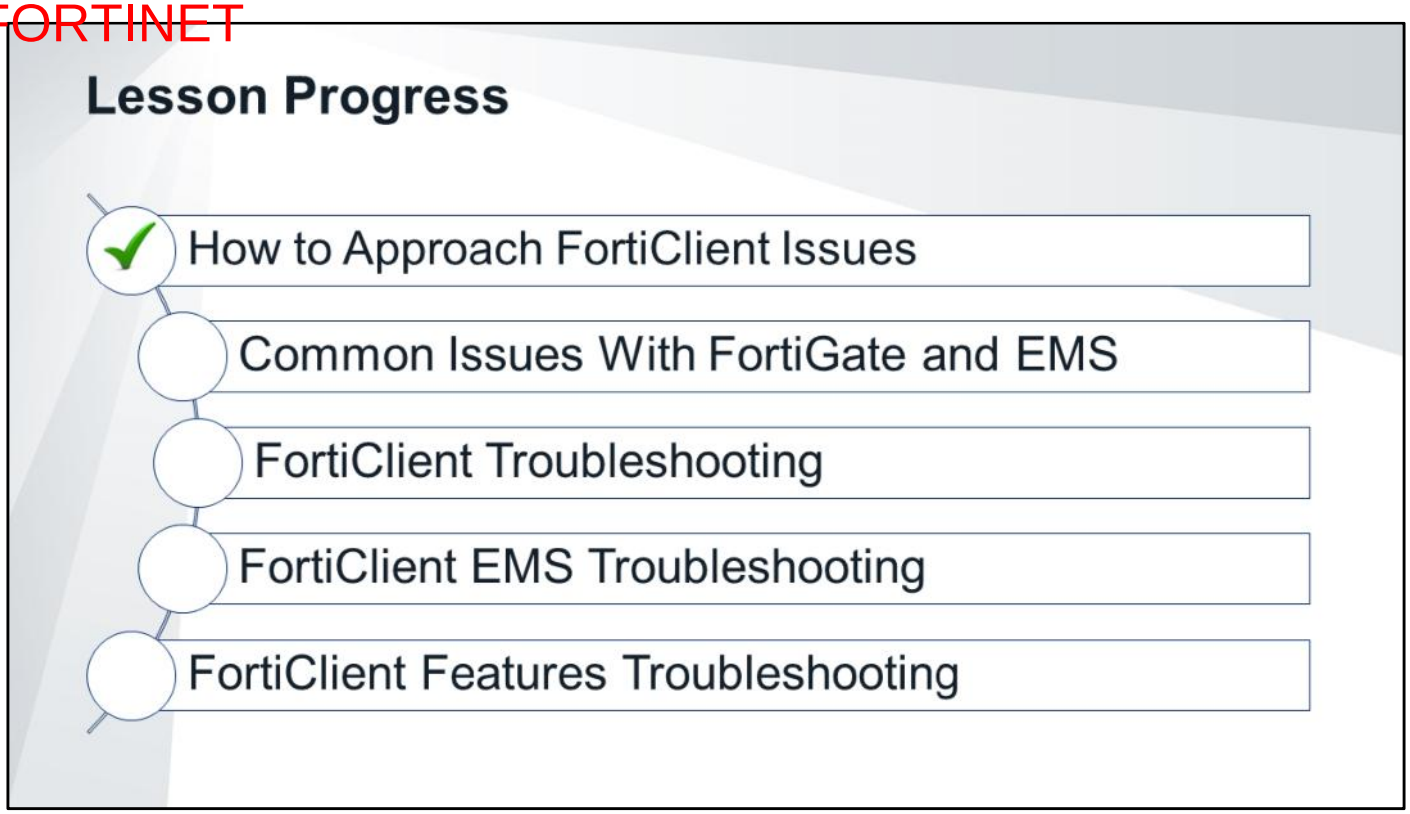
 5

The analysis phase requires testing, checking, and comparing with other users to determine if they are encountering similar issues.

Once it is determined that other users are encountering similar problems, further dissect the issue. By comparing the expected results with your results. Find out if the issue is reproducible. These actions result in a list of possible solutions that you can evaluate in the lab.

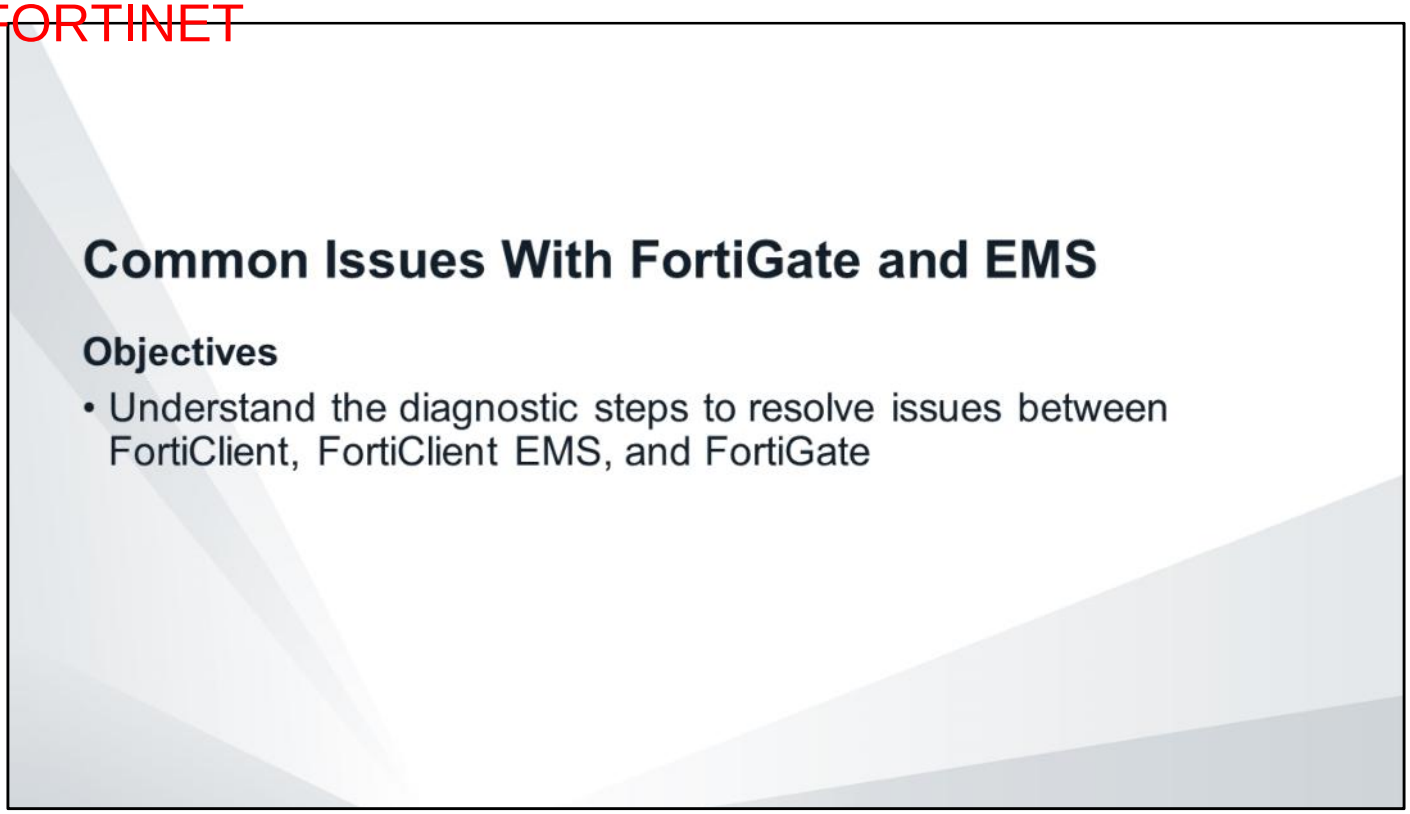
Remember, there might be multiple ways to resolve an issue. You should always document each of possible solution. You should also create a backup plan before implementing a solution, in case you need to revert to a previous state.

Once you implement a solution, monitor and review the results.



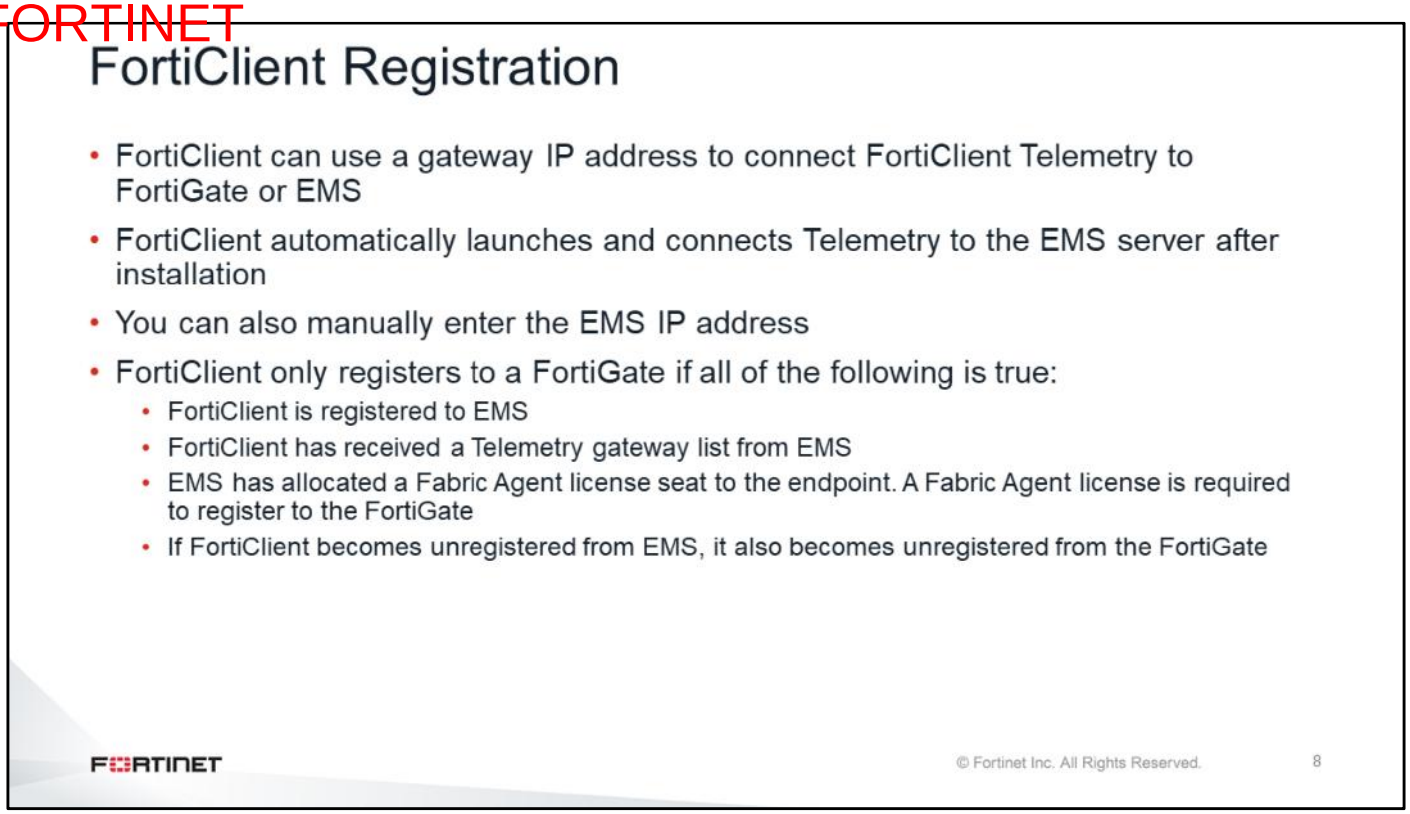
Good job! You now understand how to approach FortiClient issues.

Now, you will learn about FortiClient EMS issues.



After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in taking diagnostic steps, you will be able to diagnose and resolve common issues between FortiClient, FortiClient EMS, and FortiGate.



FortiClient can use a telemetry gateway IP address to connect FortiClient Telemetry to FortiGate or EMS. After FortiClient software installation completes on an endpoint, FortiClient automatically launches and connects telemetry to the EMS server that created the installed deployment package. You can also manually enter the EMS IP address.

FortiClient only registers to a FortiGate if all of the following is true:

- FortiClient is registered to EMS.
- FortiClient has received a Telemetry gateway list from EMS.
- EMS has allocated a Fabric Agent license seat to the endpoint. A Fabric Agent license is required to register to the FortiGate.
- If FortiClient becomes unregistered from EMS, it also becomes unregistered from the FortiGate

Note that FortiClient uses the same process to connect Telemetry to EMS after the FortiClient endpoint restarts, re-joins the network, or encounters a network change.

FortiClient and FortiGate

- Registration issues:
  - IP and listening port on FortiGate or FortiClient EMS
  - Interface setting on FortiGate
- FortiClient logs:
  - **Settings** > **Logging** > **Export logs**
- FortiGate CLI commands:
  - `diagnose endpoint record-list <ipv4-address> <any>`

Exported logs from FortiClient

```
3:41:39 PM  Debug  ESNAC  PIPEMSG_CMD_ESNAC_STATUS_REG_TO_IP
3:41:39 PM  Debug  ESNAC  bClientReg false
3:41:39 PM  Debug  ESNAC  bFirstKA true
3:41:39 PM  Debug  ESNAC  Start searching for FGT
3:41:39 PM  Debug  Scheduler      handle_processtermination() called
3:41:39 PM  Debug  Scheduler      child process terminates normally
3:41:40 PM  Debug  ESNAC  Timeout in select in SocketConnect
3:41:40 PM  Debug  ESNAC  Socket connect failed
3:41:40 PM  Debug  ESNAC  10.0.1.253:8013, Secondary - 0
3:41:40 PM  Debug  ESNAC  CKeepAlive::SetState
3:41:40 PM  Debug  ESNAC  Not Registered
3:41:40 PM  Debug  ESNAC  m_dwAutoconnectWhenOffnet false
3:41:40 PM  Debug  ESNAC  CKeepAlive::SetState
3:41:40 PM  Debug  ESNAC  FortiGate not Found
3:41:40 PM  Debug  ESNAC  The state has changed
3:41:40 PM  Debug  ESNAC  End searching for FGT
```

```
FGVM010000052731 # diagnose endpoint record-list
Record #1:
                IP Address = 10.0.1.10(1)
                MAC_Address = 00:0c:29:5c:25:17
                Host MAC_Address = 00:0c:29:5c:25:17
                MAC list = 00-0c-29-5c-25-17;d8-9c-67-9e-e5-d2;
                VDOM = root
                EMS serial number: FCTEMS0000100991
                Quarantined: no
                Online status: online
                On-net status: on-net
                FortiClient connection route: Direct
                FortiClient communication interface index: 4
                DHCP server:
                Dirty_onnet_addr: yes
                FortiClient version: 6.2.1
                AVDB version: 73.396
                FortiClient app signature version: 15.734
                FortiClient vulnerability scan engine version: 2.28
                FortiClient feature version status: 0
                FortiClient UID: 0FFD3656F1ED495BADC7E2A6E20EEF0C (0)
                FortiClient KA interval dirty: 0
                FortiClient Full KA interval dirty: 0
                Auth_AD_groups:
                Auth_group:
                Auth_user: ADMIN
                Host_Name: DESKTOP-8K1R2V5
                OS_Version: Microsoft Windows 10 Enterprise Edition, 64-bit (build 10240)
```

FORTINET

9

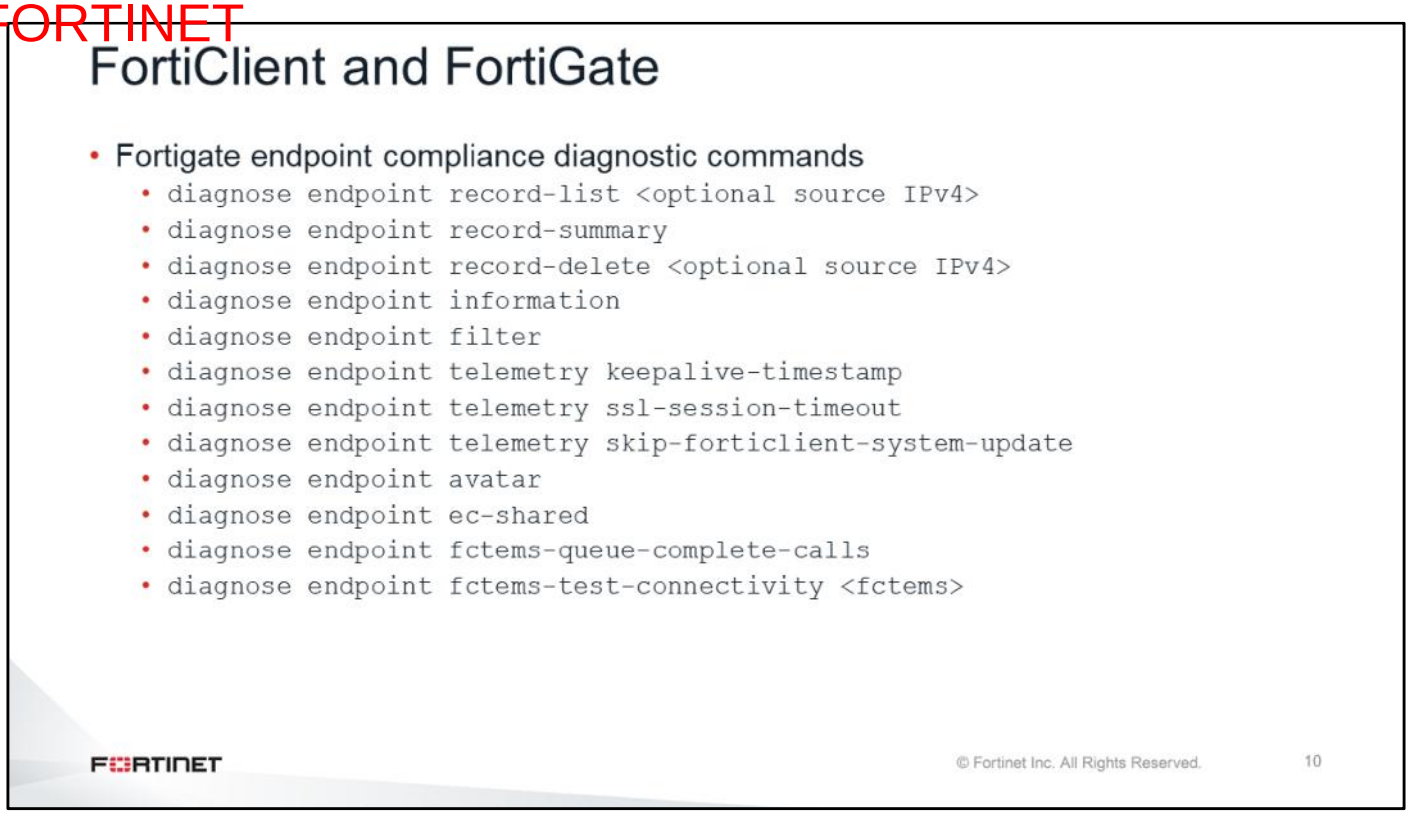
If FortiClient is not able to register to on FortiGate, make sure that the firewall or another program is not blocking the FortiGate interface IP and port 8013. Check the interface setting on FortiGate to make sure **FortiTelemetry** is enabled on the interface.

In the example logs shown on this slide, **FortiTelemetry** is not enabled on FortiGate and, because of that, FortiClient is not able to find FortiGate. You can capture packets on the local PC to make sure packets are routed toward FortiGate, or run the sniffer on FortiGate to verify the traffic flow. Make sure to check the interface settings on the FortiGate.

Once FortiClient access is enabled, FortiClient detects FortiGate and preregisters on FortiGate, whereas FortiGate verifies, registers, and applies the correct FortiClient profile.

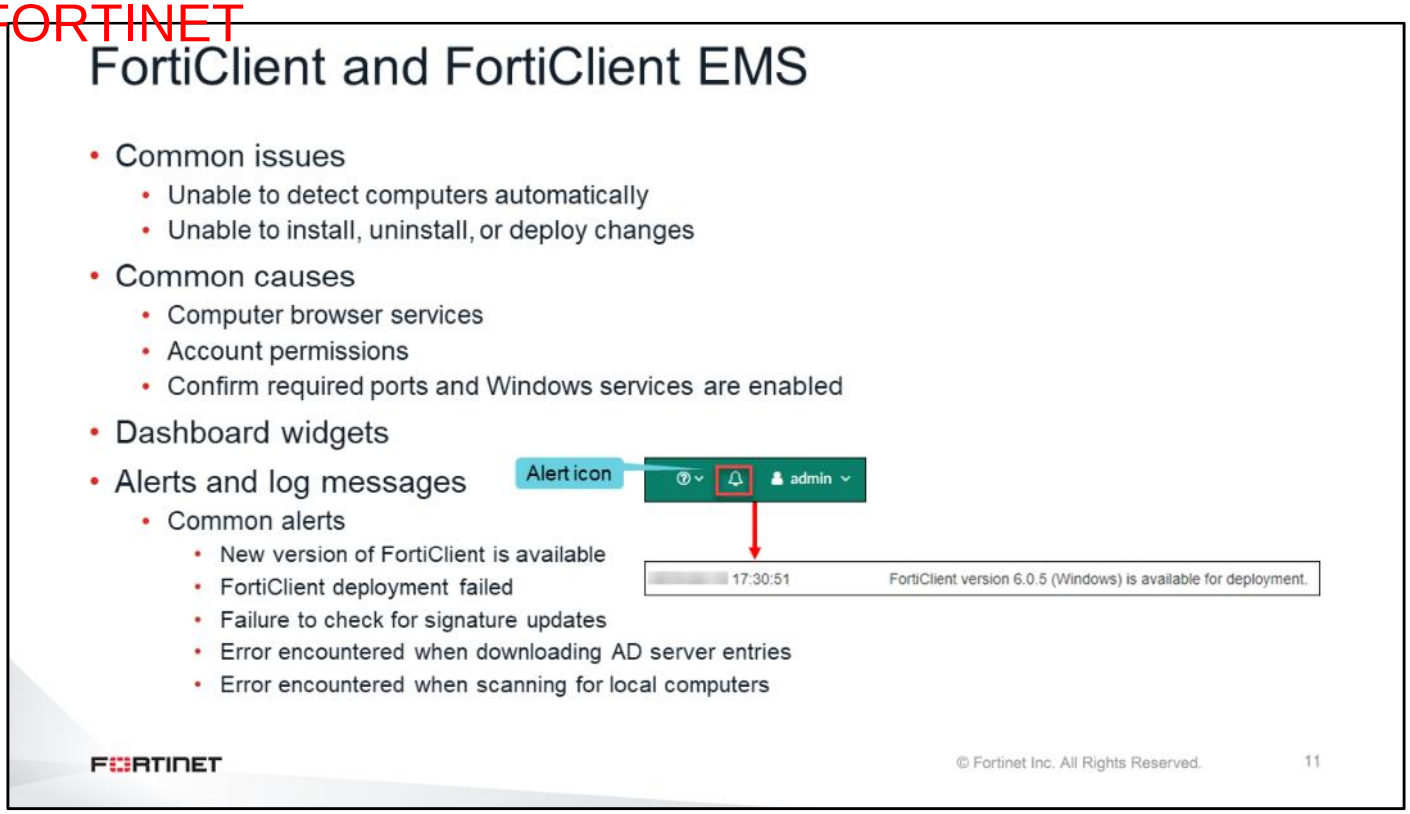
You can run endpoint commands to verify the endpoint record and registration on FortiGate.

The `diagnose endpoint record-list` command provides the IP address, online status, user, host OS, and so on, for the FortiClient endpoint.



This slide shows some other useful CLI diagnostic commands on FortiGate. Here is the description of all the commands:

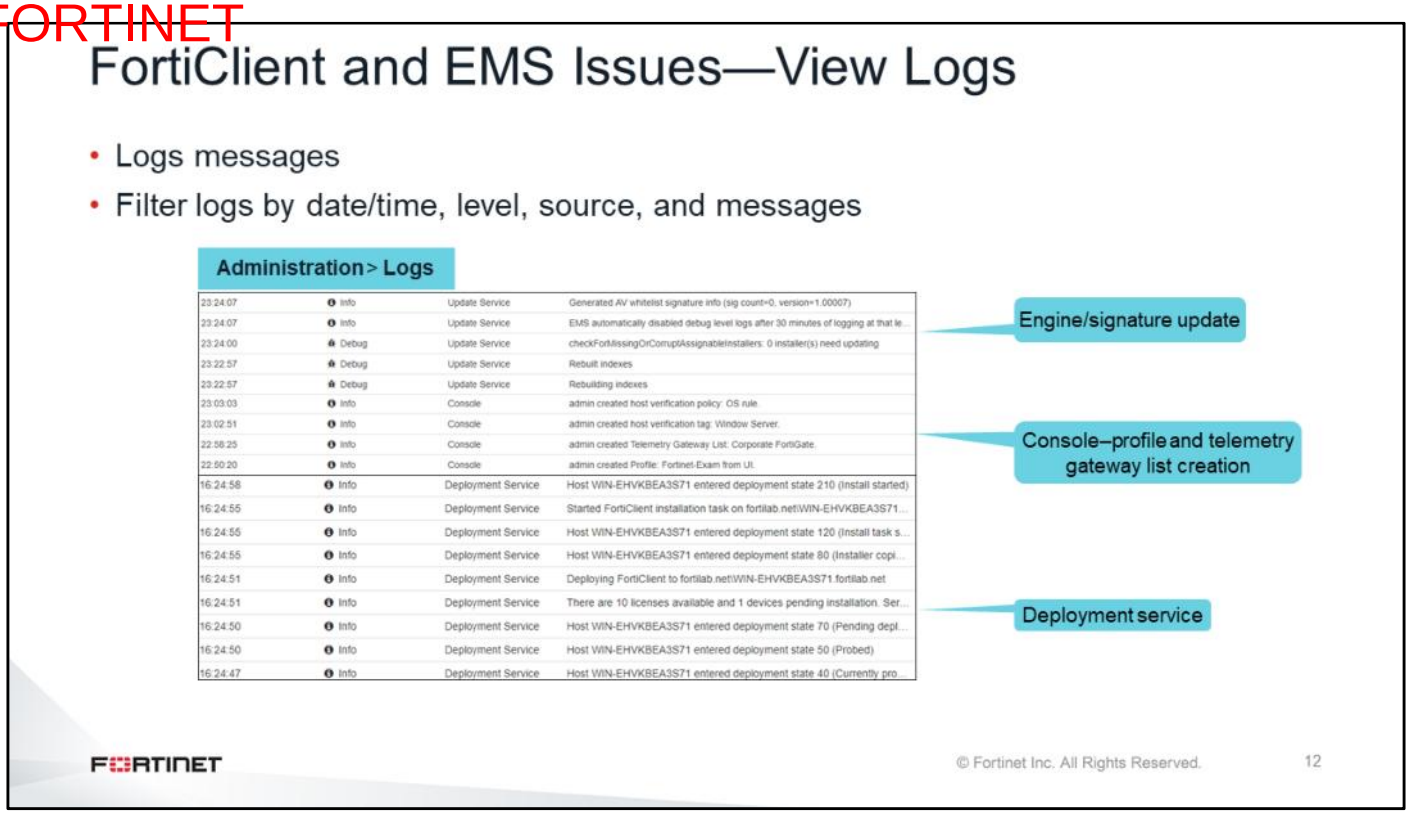
- `record-list` command lists endpoint records.
- `record-summary` command lists the summary of endpoint records.
- `record-delete` command deletes endpoint records.
- `Information` command displays latest endpoint related information.
- `Filter` command applies debug filter to fcnacd process.
- `avatar` command displays FortiClient avatar.
- `ec-shared` command displays FortiClient shared record.
- `fctems-queue-complete-calls` command adds complete (un)quarantine call(s) to FCNACD EMS queue.
- `fctems-test-connectivity` command is used to do connectivity test for FortiClient EMS.



Multiple dependencies and various factors can be involved when troubleshooting FortiClient and FortiClient EMS issues. Common issues can be that FortiClient is unable to automatically detect any computer running Microsoft Windows, that you are unable to install or uninstall FortiClient from the host machine, or that you are unable to deploy changes using FortiClient EMS. You can resolve these issues by verifying the computer browser services, account permissions, and ports and services enabled for EMS.

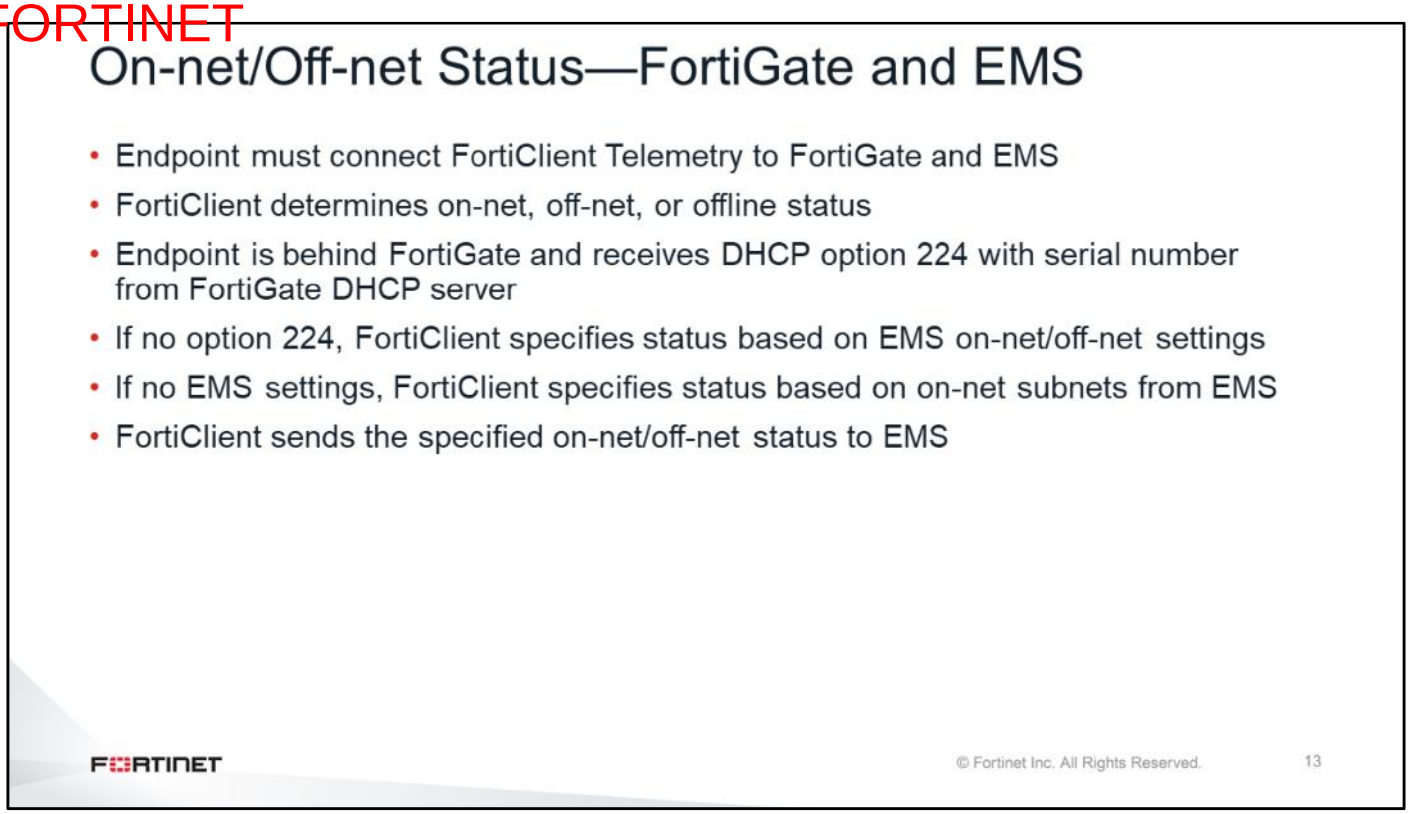
1. Computer browser services automatically detects Microsoft Windows computers within the same local network. Make sure computer browser services are running. For example, if the FortiClient EMS is installed on Windows 2012 R2, on which, computer browser service is disabled by default, FortiClient EMS will not detect computers on the same network, even if they are available.
2. Account permissions are required. Make sure the server and client have the correct account permissions to deploy the changes. For example, the administrator needs the correct permissions to create or deploy the changes on FortiClient EMS.
3. Confirm required ports and Windows services are enabled on EMS. FortiClient EMS uses many ports and services in order to communicate with clients and servers running associated applications. Make sure these ports and services are enabled for use for FortiClient EMS. On the client side, make sure **Task Scheduler** is set to **Automatic**, **Windows Installer** is set to **Manual**, and **Remote Registry** is set to **Automatic**.

FortiClient EMS has several dashboard widgets that provide information about managed clients and their current statuses. You can view alerts generated by FortiClient EMS by clicking the bell icon in the toolbar, which shows you generated alerts. An example of a common alert is “New version of FortiClient is available”. Note that configuration changes to FortiClient are always pushed by EMS. FortiClient only send telemetry data for status updates.



You can view the logs on FortiClient EMS using the **Logs** page. You can filter logs by using various parameters, such as date/time, log level, source (such as **EMS Service**, **Update Service**, **AD Service**), and messages.

In the example shown on this slide, the logs provide detailed messages about the event occurred, which you can use to troubleshoot the issues with FortiClient and FortiClient EMS. You should change the log level to **Debug**.



When FortiClient connects Telemetry to EMS and to FortiGate, FortiClient calculates on-net/off-net information. The following examples show how FortiClient determines the endpoint status:

- The endpoint has an on-net status when the endpoint is behind a FortiGate and receives option 224 with the FortiGate serial number. In this case, FortiGate is the DHCP server, and FortiGate checks that the serial number matches its own serial number.
- If option 224 is not received or there is no match with the currently registered serial number, FortiClient determines on-net/off-net status based on the DHCP on-net/off-net setting in EMS.
- If there is no EMS setting, FortiClient determines on-net/off-net status based on the on-net subnets received from EMS.
- FortiClient sends the specified on-net/off-net status to EMS.

Note that you must remove the `on-net` subnet setting from FortiClient XML manually, before configuring `on-net` using EMS. When FortiGate and EMS are integrated, the primary FortiClient Telemetry connection is to FortiGate, and FortiGate calculates the status.

On-net/Off-net Status—EMS Only

- FortiClient EMS only
- The following table shows how various configurations specify the endpoint status:

EMS DHCP onnet/offnet setting	EMS On-net Subnets setting	Option 224 serial number	Resulting endpoint status
Disabled	Disabled	N/A	When on-net subnets are not configured, on-net/offnet status is related to the endpoint's online/offline status (whether it is connected to EMS). An online status causes the endpoint to be on-net, while an offline status causes the endpoint to be off net.
Enabled	Disabled	Not configured	Same as above
Enabled	Disabled	Configured	On-net Since Option 224 is configured with a Fortinet device's serial number, EMS assumes FortiClient is on-net with that FortiGate.
Disabled or enabled	Enabled, with subnet configured. Endpoint IP address is in the configured subnet.	Configured or not	On-net The endpoint is inside the on-net networks configured in *On-Net Subnets*.
Disabled or enabled	Enabled, with subnet configured. Endpoint IP address is not in the configured subnet.	Configured or not	Off-net The endpoint is outside the on-net networks configured in *On-Net Subnets*

FORTINET

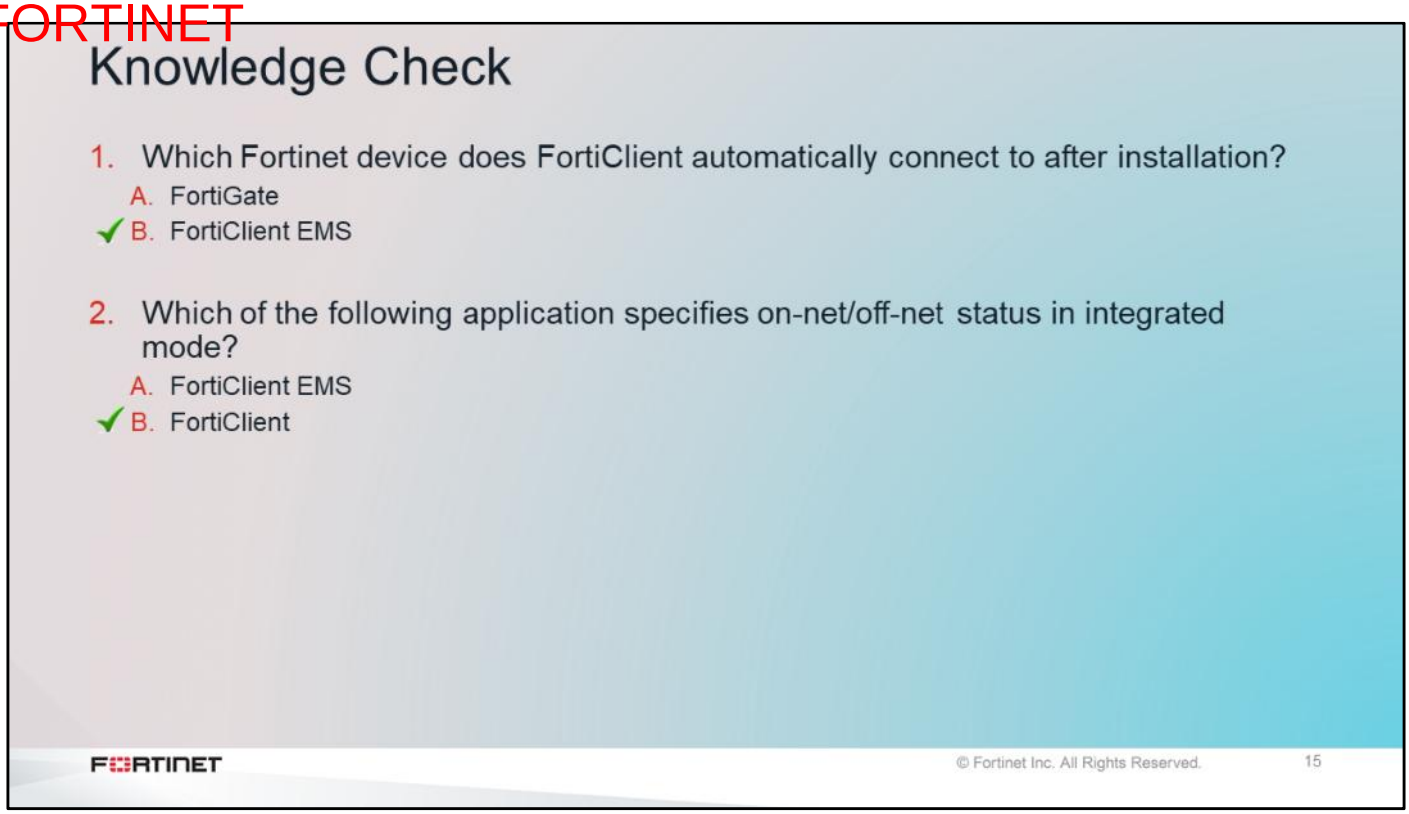
14

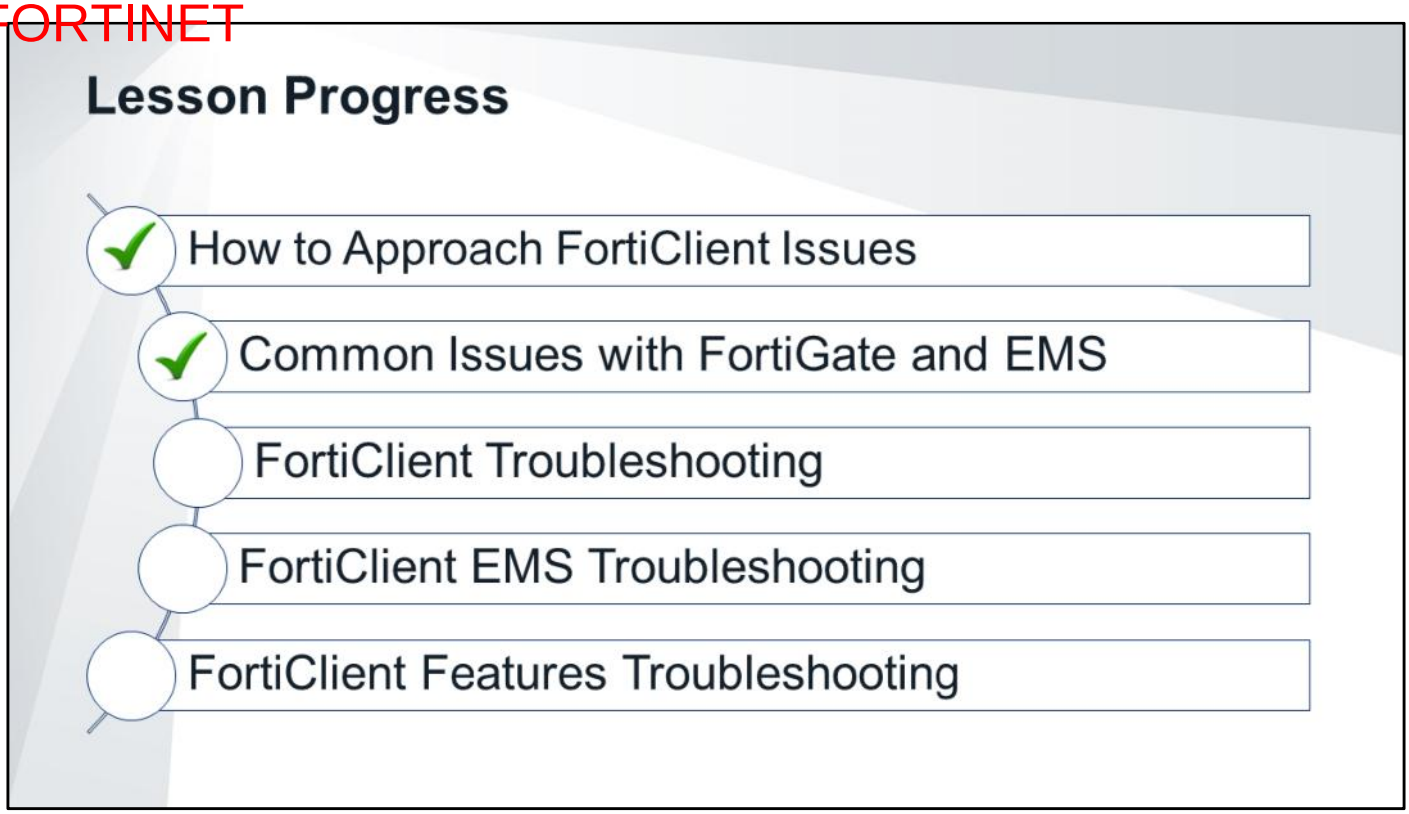
When FortiClient connects Telemetry to EMS only, **DHCP onnet/offnet** and **on-net Subnets** settings in EMS affect on-net/off-net status. The table on this slide shows how various configurations specify the endpoint status when FortiClient Telemetry is connected to EMS.

The following examples show how endpoint status is specified when FortiClient is connected to EMS only:

- The endpoint has an offline status when the endpoint cannot connect FortiClient Telemetry to EMS and is outside one of the on-net networks
- The endpoint has an offline on-net status when the endpoint cannot connect FortiClient Telemetry to EMS but is inside one of the on-net networks

Note that on-net subnets have higher priority over other settings. In addition, EMS does not compare the option 224 serial number. As long as the endpoint has the serial number, EMS assumes the endpoint is behind FortiGate and is on-net.



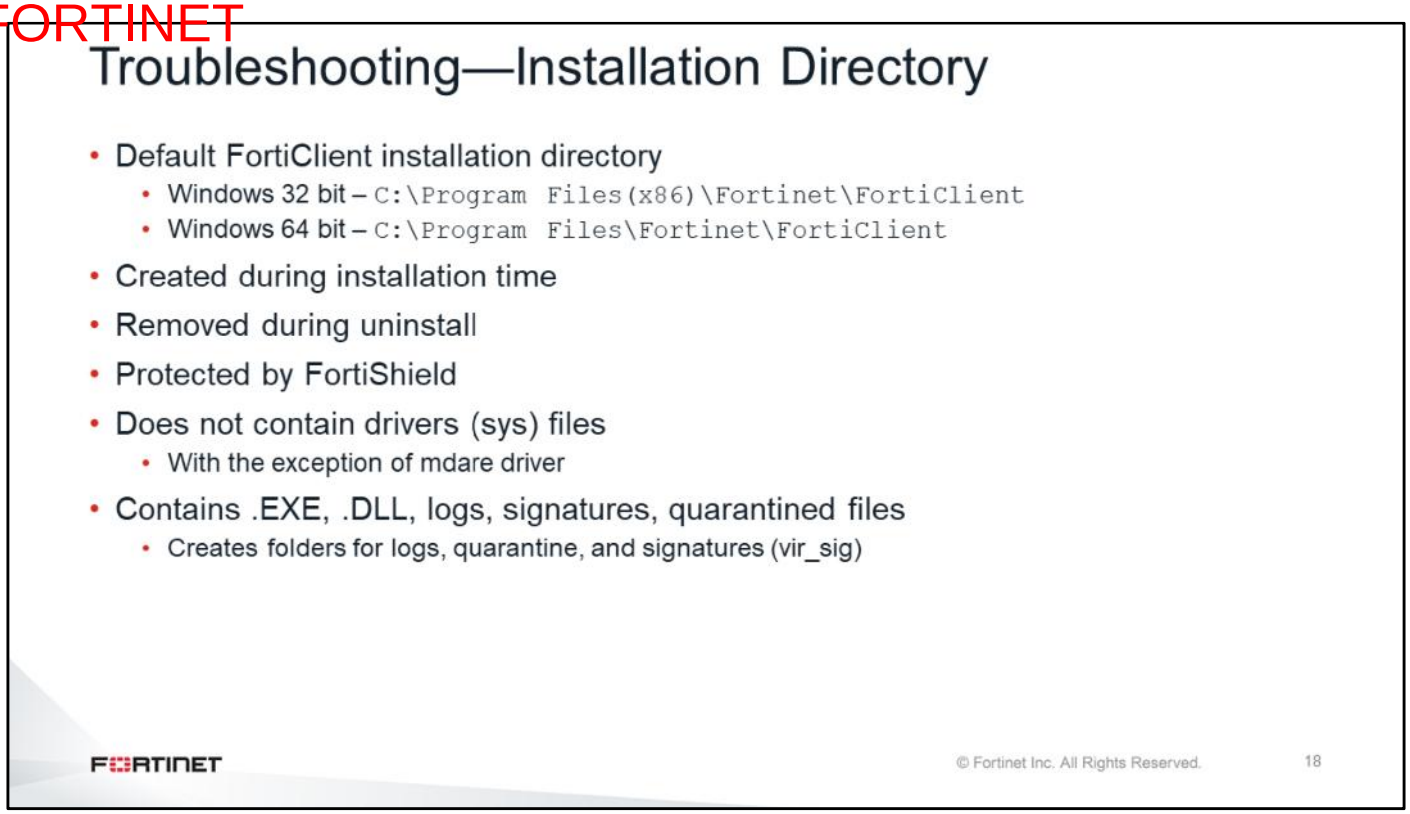


Good job! You now understand the diagnostics steps involved in resolving common issues between FortiClient and FortiClient EMS.

Now, you will learn about FortiClient components and troubleshooting.

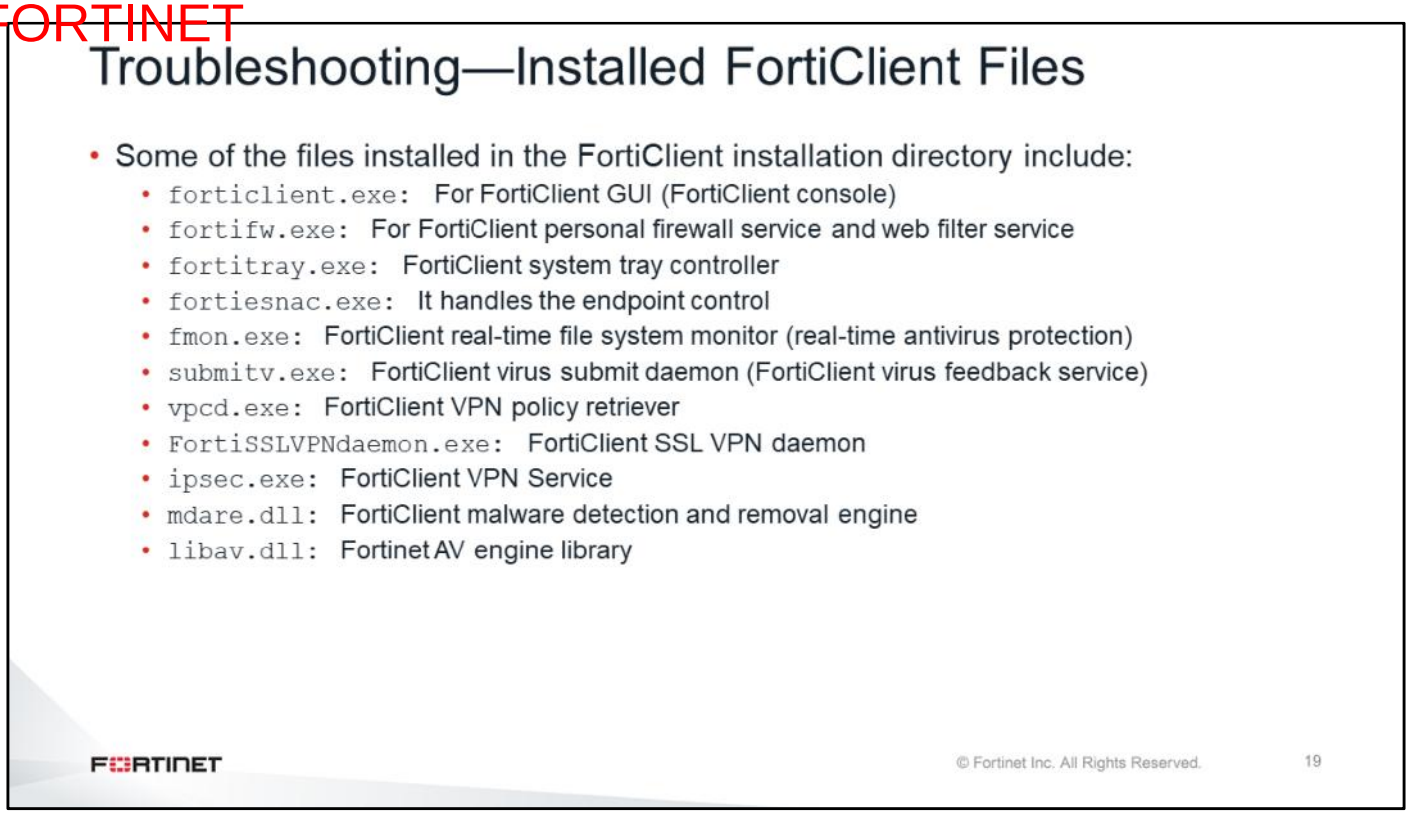
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in FortiClient components and troubleshooting, you will be able to resolve issues on the Windows operating systems.

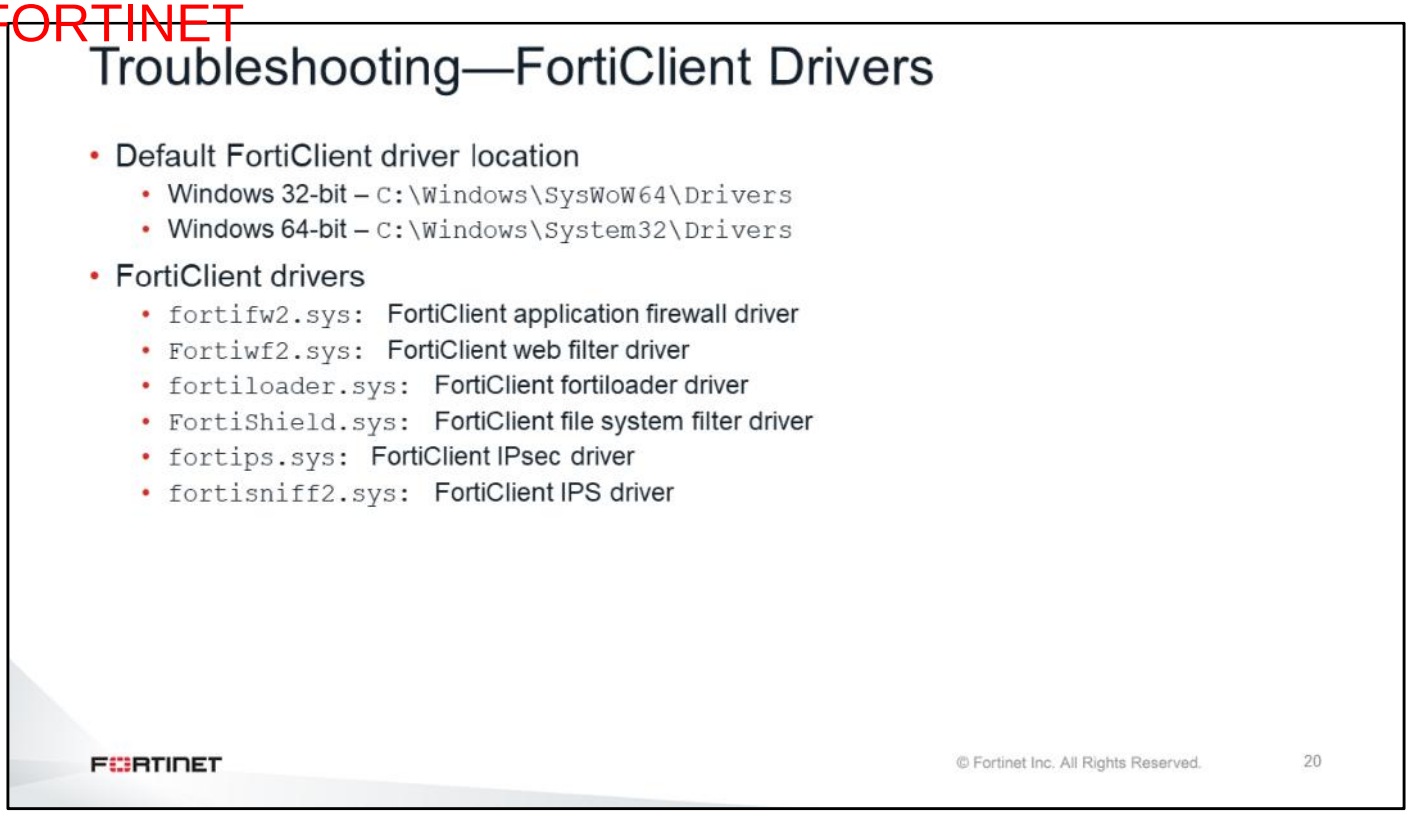


When FortiClient is installed on Windows OS, by default it is installed in `Program Files` on Windows 32-bit OS, and `Program Files (x86)` on Windows 64-bit OS. The FortiClient directory is created only during installation and removed during uninstallation.

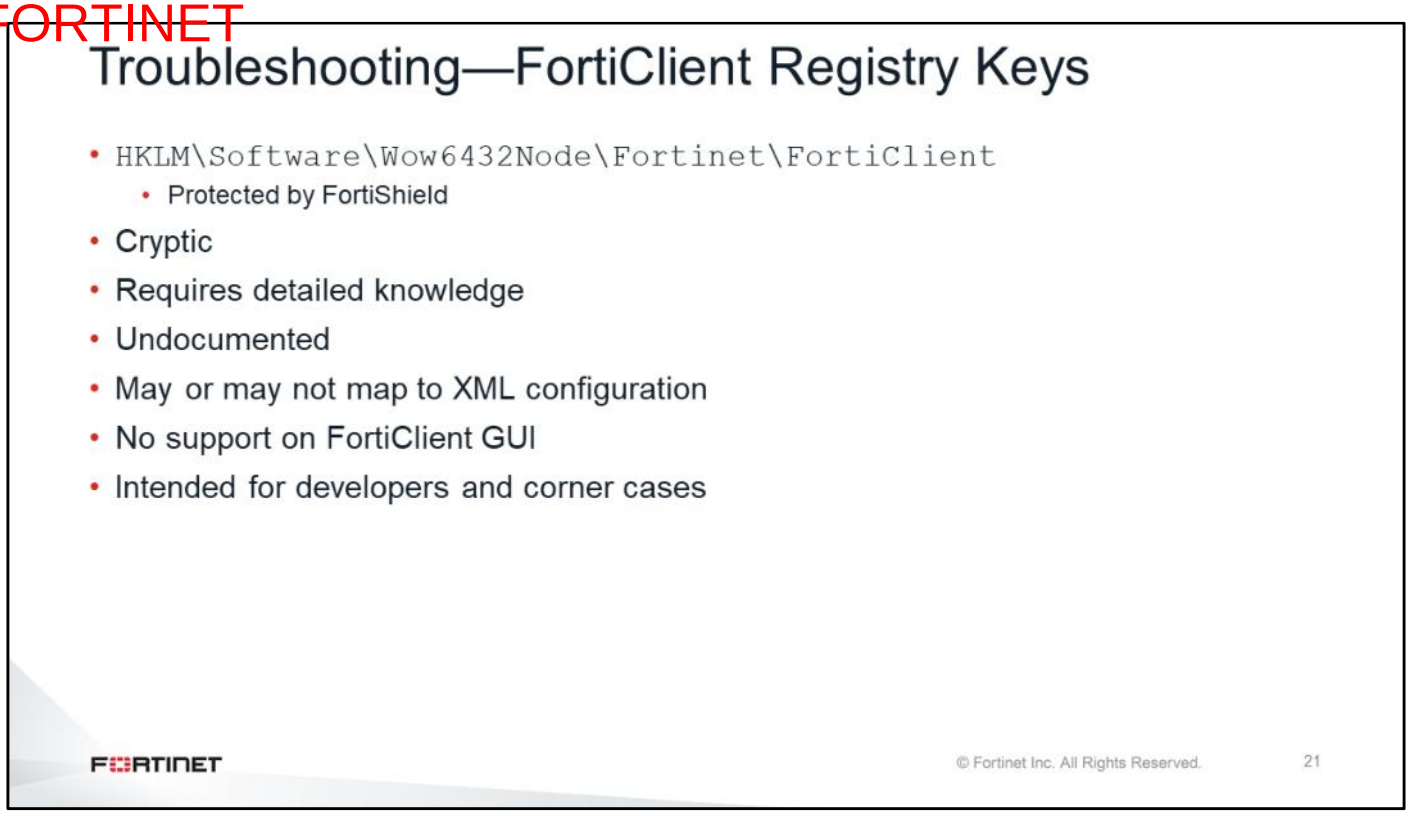
You can change the default installation directory while installing FortiClient. FortiClient is protected by FortiShield, which is digitally signed and prevents modification of the Windows registry. The FortiClient folder contains .EXE files, .DLL files, logs, signatures, quarantine files, and so on.



When you install FortiClient, it installs a number of executables, DLL files, signatures, and so on. Refer to this slide for the list of FortiClient executable files and descriptions.



When FortiClient is installed on Windows OS, it installs the necessary drivers on Windows 32-bit OS and Windows 64-bit OS. Refer to this slide for the list of FortiClient drivers and descriptions.



You can check the FortiClient registry keys at location show in this slide. The registry keys are protected by FortiShield.

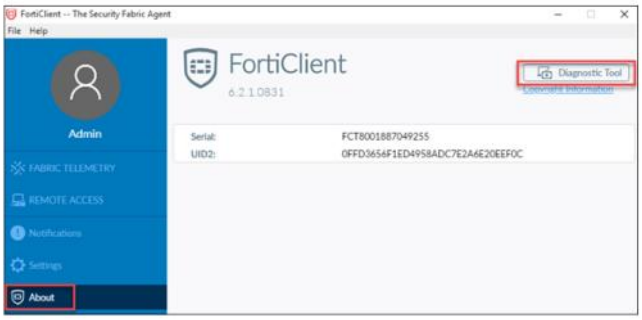
Unlike XML, registry keys are cryptic and the user requires detailed knowledge to configure. The keys can't be documented in any format and so they are not supported on the FortiClient GUI. The keys are intended for use by developers.

Note that in some cases, Fortinet support can ask you to change the FortiClient registry or replace FortiClient files. To perform this task, you must stop FortiShield first:

- Disconnect FortiClient from EMS
- Shut down FortiClient
- In an elevated command-line window, type `sc stop fortishield`

Troubleshooting—Diagnostic Tool

- You can access the FortiClient Diagnostic Tool on the FortiClient console
  - Click **About**
- FortiClient Diagnostic Tool generates a debug report
- FortiClient Diagnostic Tool does not record sensitive information
- It contains the following information about the endpoint:
  - Windows operating system version
  - Windows software updates
  - Names and versions of installed software
  - Names and versions of installed drivers
  - FortiClient configuration
  - FortiClient logs



FORTINET

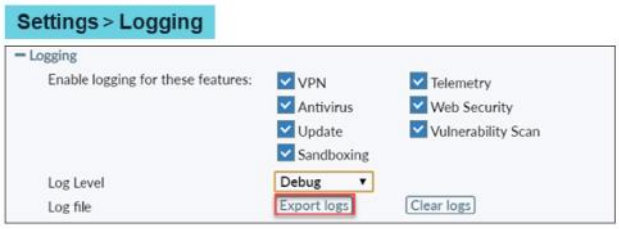
22

You can use the FortiClient Diagnostic Tool to generate a debug report, and then provide the debug report to the FortiClient team to help with troubleshooting. For example, if you are working with customer support on a problem, you can generate a debug report, and send the report to customer support to help with troubleshooting.

The FortiClient Diagnostic Tool does not record sensitive information. It contains information about the endpoint that are shown in this slide.

Troubleshooting—Logs

- You can export logs from FortiClient to review
- Change log level
  - To troubleshoot, you must change log level to **Debug**
- Default log level is **Information**



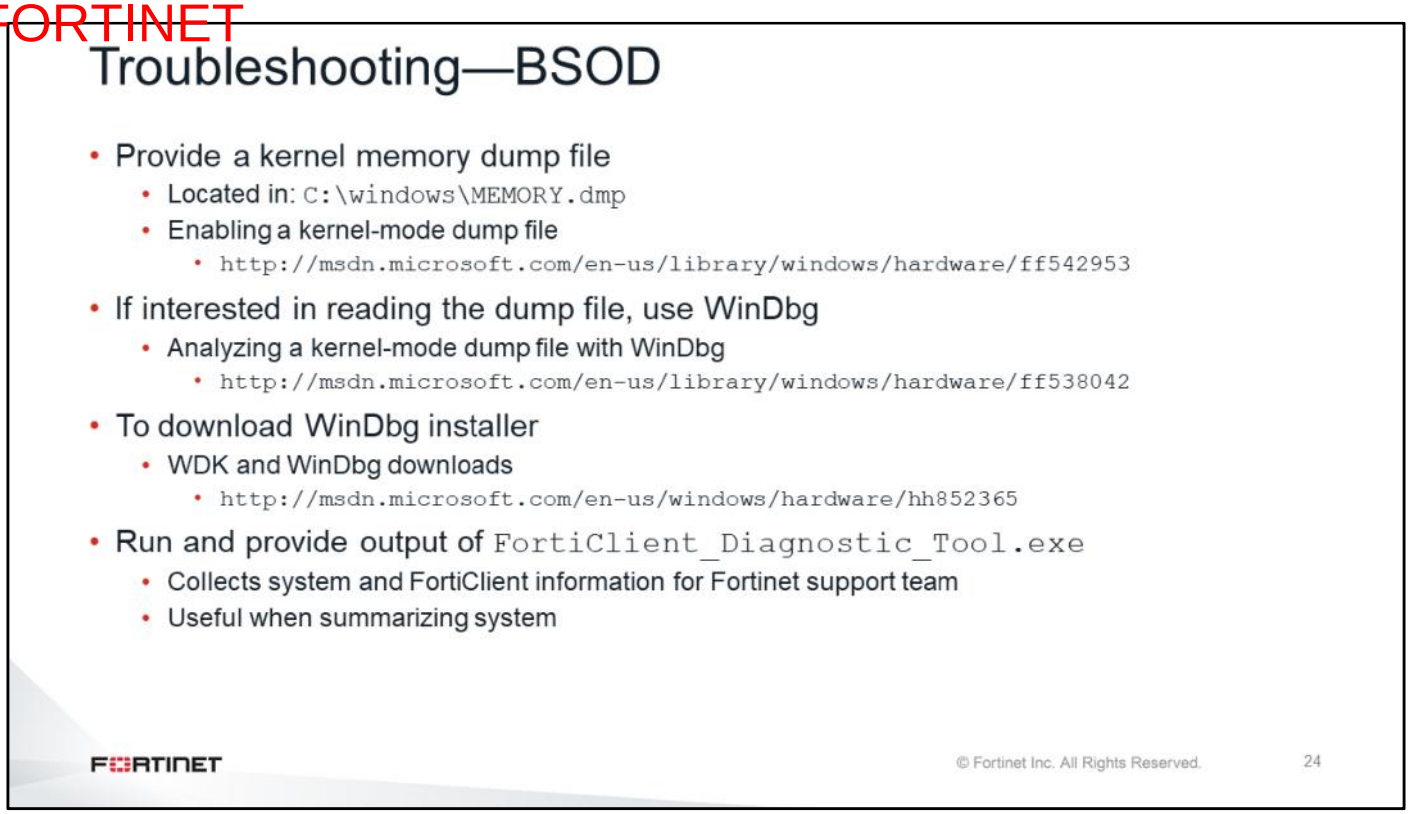
FORTINET

23

By default, the log level is set to **Information**, which provides enough related information to resolve common FortiClient issues. However, you can change the log level on EMS, and you can send the necessary configuration from **System Settings** page to FortiClient.

There are various log levels on FortiClient, such as **Emergency**, **Alert**, **Information**, **Debug**, and so on. To get more detailed logs for debugging, change the log level to Debug.

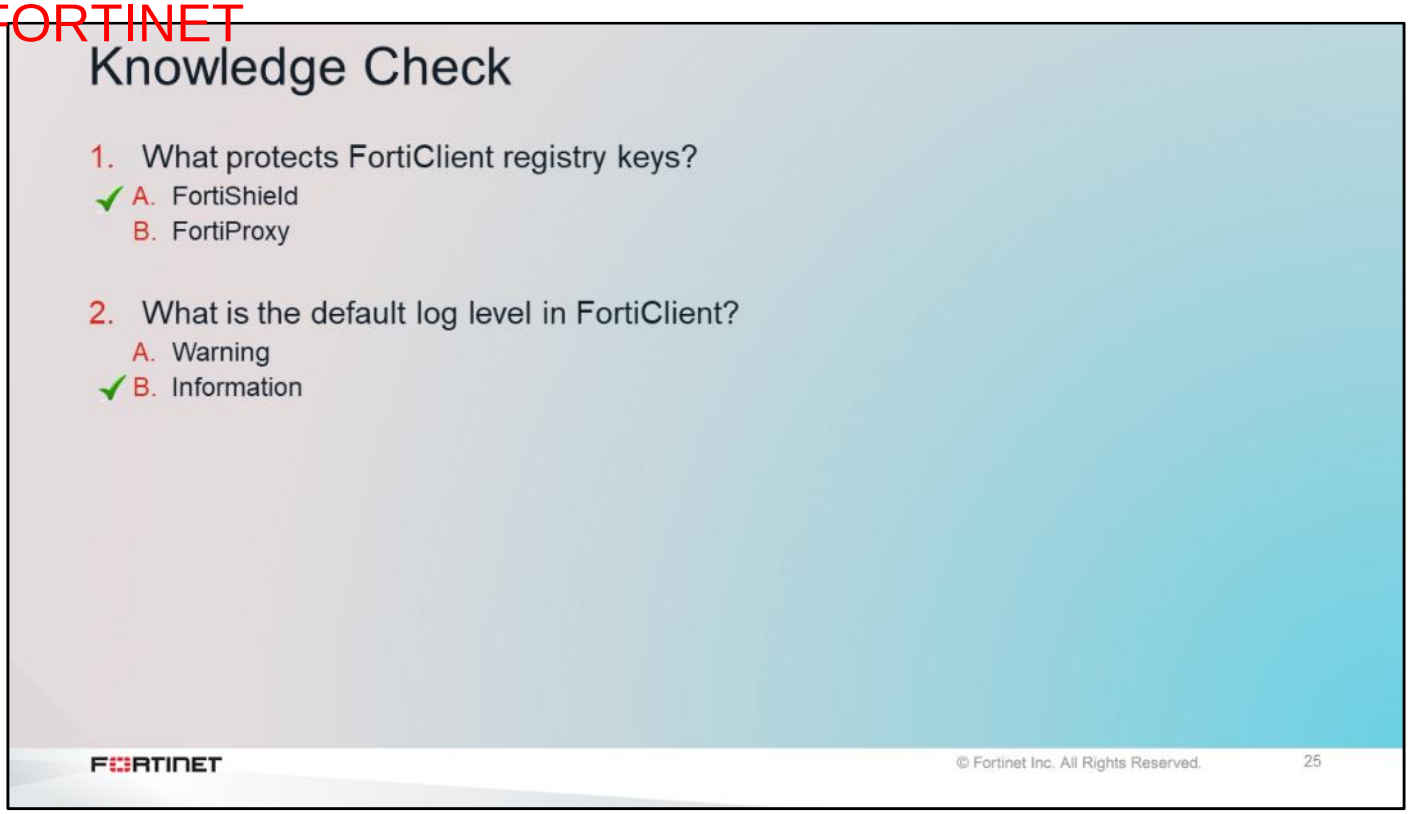
Note that you can clear the check boxes next to features to reduce log entries when troubleshooting a specific feature issue.

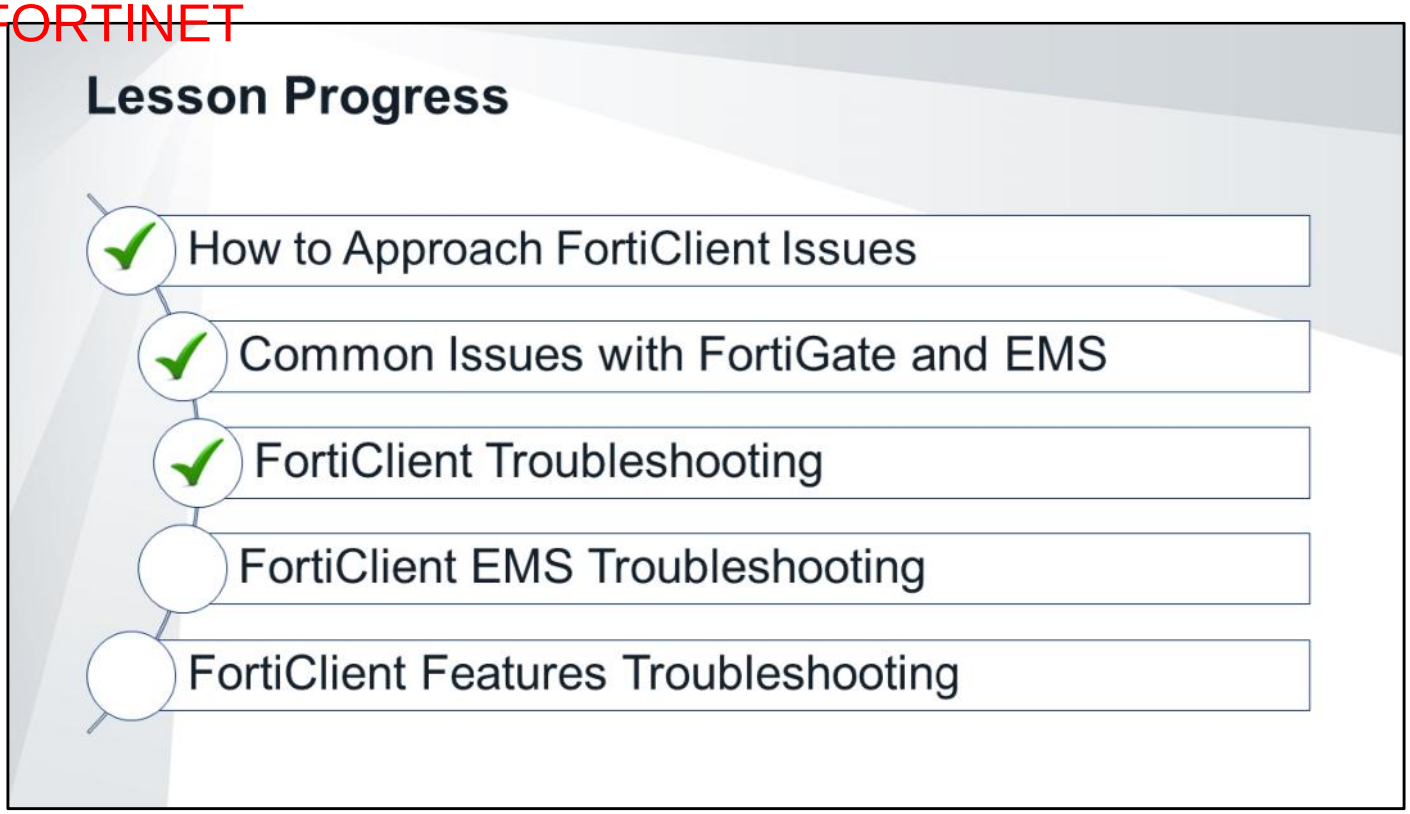


FortiClient can cause blue screen of death (BSoD) when it conflicts with third-party software. If this happens, provide a kernel memory dump. It is usually located in Windows folder as shown in this slide.

To configure the collection of dump files, refer to the Microsoft documents links that are shown on this slide.

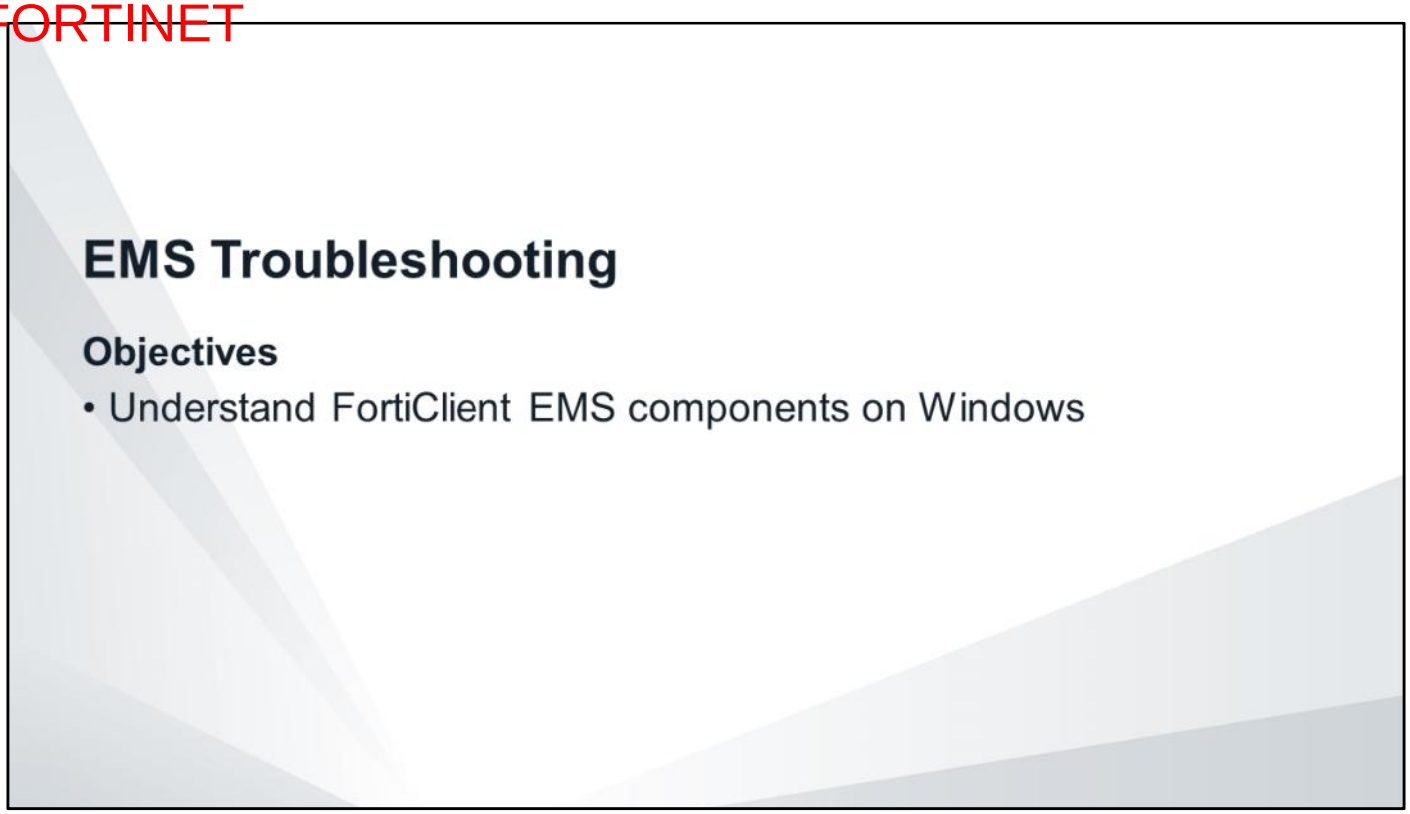
Run and provide the output of `FortiClient_Diagnostic_Tool.exe`. You can download the tool from Fortinet support website.





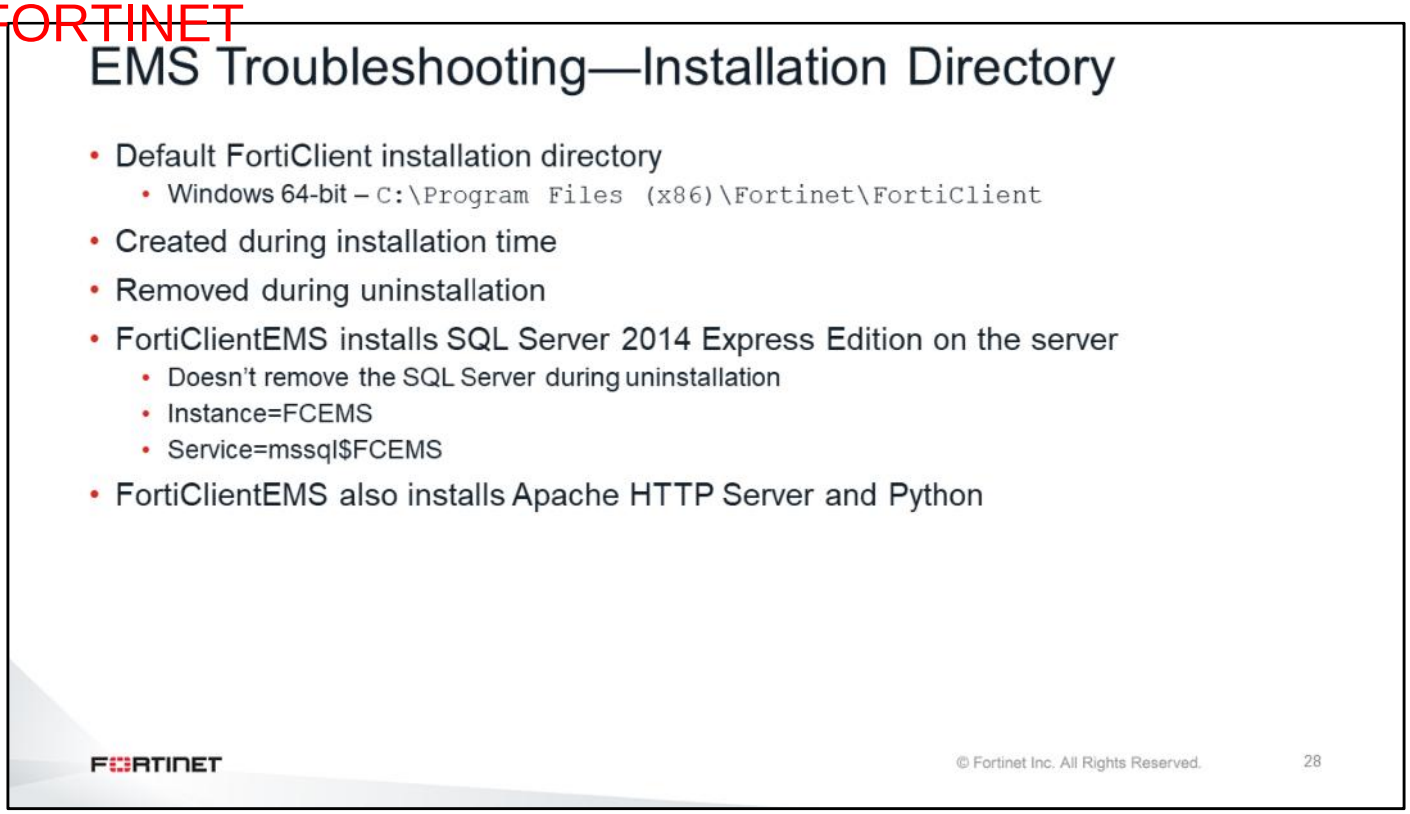
Good job! You now understand FortiClient components and troubleshooting on Windows operating systems.

Now, you will learn about FortiClient EMS troubleshooting.



After completing this section, you should be able to achieve the objectives shown on this slide.

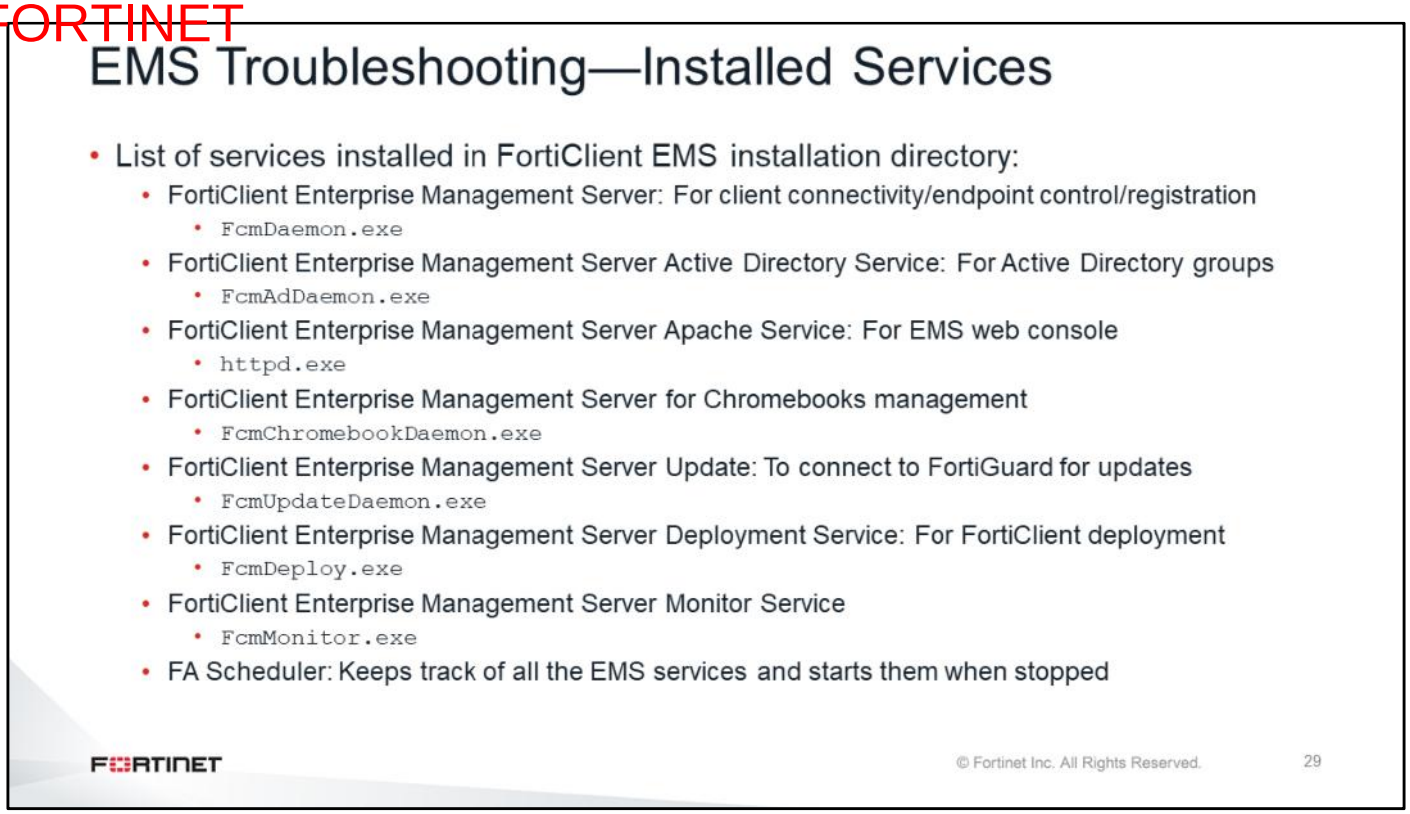
By demonstrating competence in FortiClient EMS components and troubleshooting, you will be able to resolve EMS issues on Windows servers.



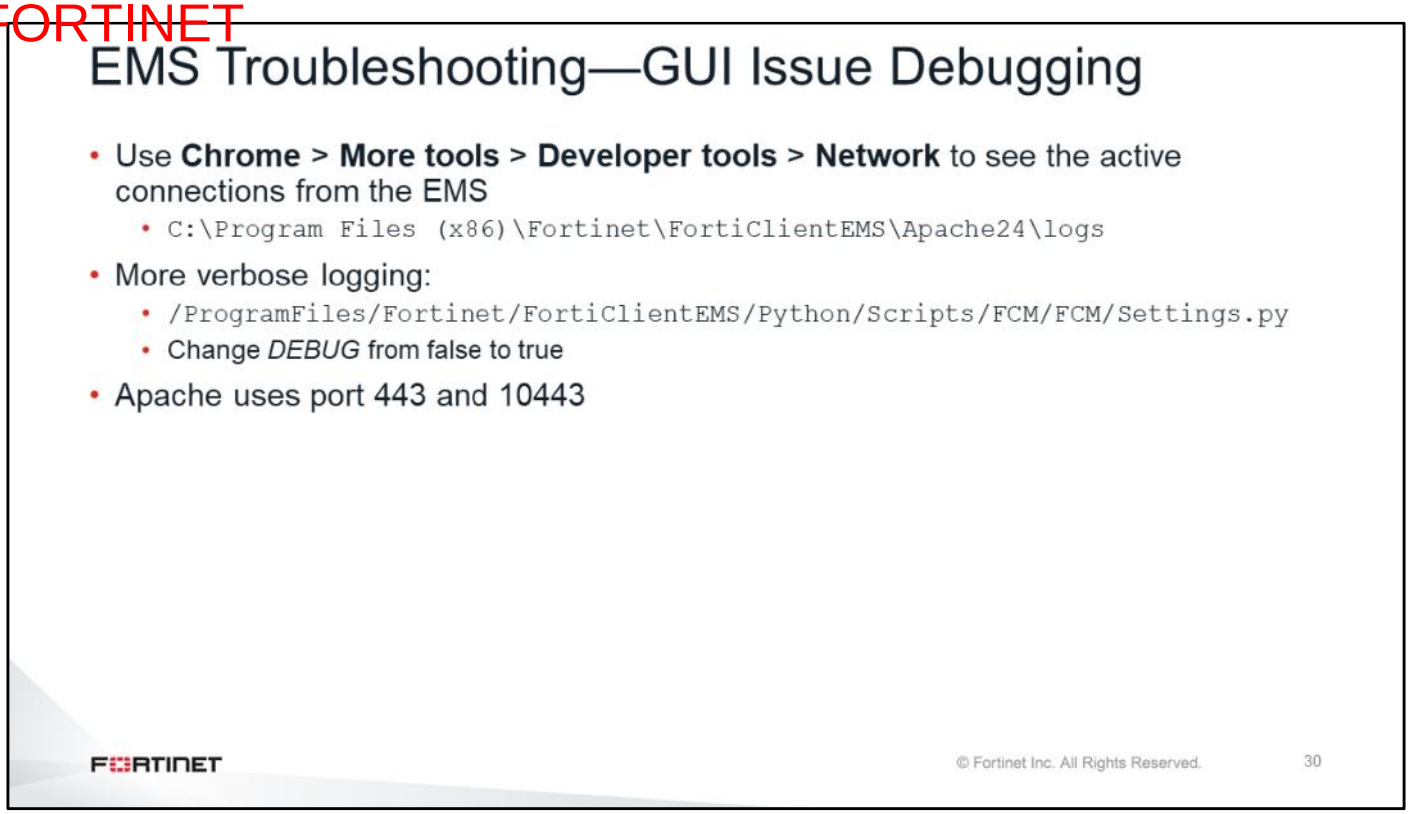
By default, FortiClient EMS is installed in Windows `Program Files (x86)` on the Windows 64-bit OS. The FortiClient EMS directory is created only during installation and is removed during uninstallation.

You can change the default installation directory while installing FortiClient EMS. FortiClient EMS installs SQL Server 2014 Express edition on the server. FortiClient EMS doesn't remove SQL Server during uninstallation.

FortiClient EMS also installs Apache HTTP Server and Python.



When you install FortiClient EMS, it installs a number of executables, dll, signatures, and so on. Refer to this slide for the list of executable files and descriptions.



You can debug GUI access issues either by using a web browser or enabling verbose logging for Python.

Make sure you turn off the debug after troubleshooting. You should not run the debug in a production environment. By default, Apache uses port 443 and 10443. You can use the `netstat` command to see if the default Apache ports are being used by another application.

EMS Troubleshooting—View Debug Logs

- You can check logs on FortiClient EMS GUI

- Change log level to **Debug**
- However this doesn't include FortiClient EMS installation logs
- For FortiClient EMS installation issues go to:
  - C:\Users\Administrator\AppData\Local\Temp\FortiClient_Enterprise
- SQL Server installation logs
  - %temp%\sql

FORTINET

31

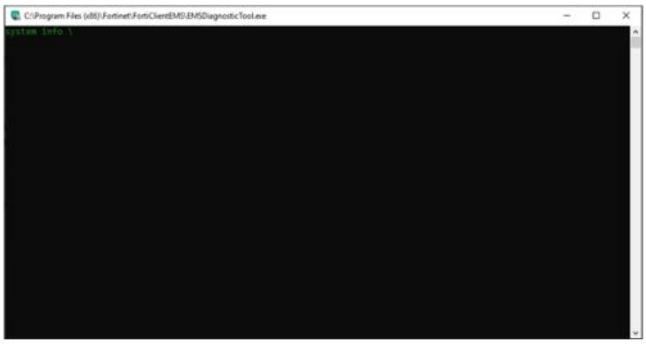
On FortiClient EMS, you can see the logs on **Logs** page. To get more information, you should to change the log level to **Debug**. However this GUI log doesn't include FortiClient EMS and SQL installation logs. Installation logs are generally available in the temp folder.

Note that FortiClient EMS automatically reverts the log level from **Debug** to **Info** after 30 minutes to save resources on the server. The FortiClient EMS GUI only displays logs from the database; daemon debug logs are sent to the file only.

EMS Troubleshooting—Diagnostic Tool

- You can access the EMS Diagnostic Tool in:
  - C:\ProgramFile(x86)\Foritnet\FortiClientEMS

- FortiClient EMS Diagnostic Tool generates a debug report
- FortiClient Diagnostic Tool does not record sensitive information
- It contains the following information about the endpoint:
  - Windows operating system version
  - Server event logs
  - FortiClient EMS Apache configuration
  - FortiClient EMS Apache logs
  - FortiClient EMS logs
  - Names and versions of installed software
  - Names and versions of installed drivers
  - Python logs
  - Temp directory installation logs

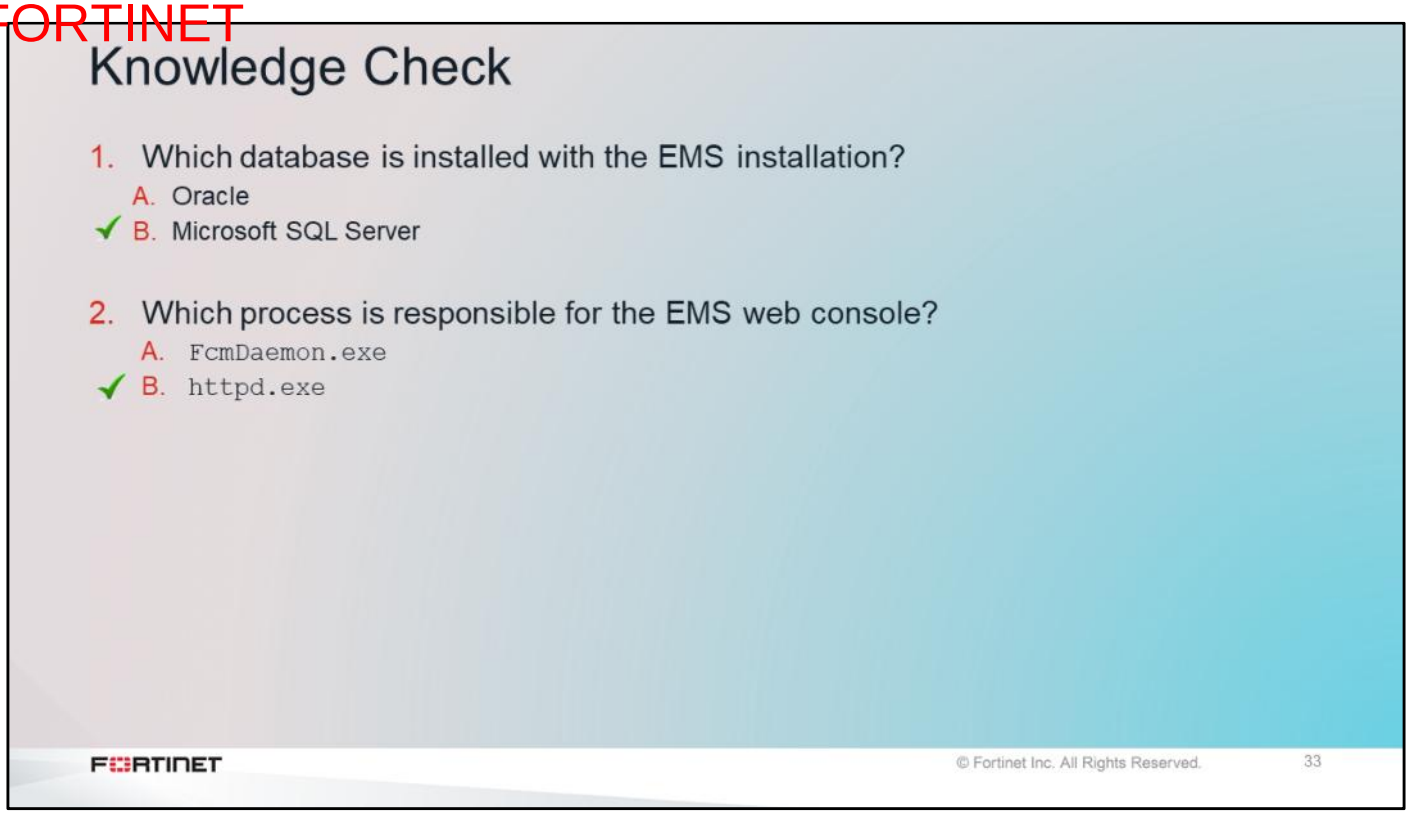


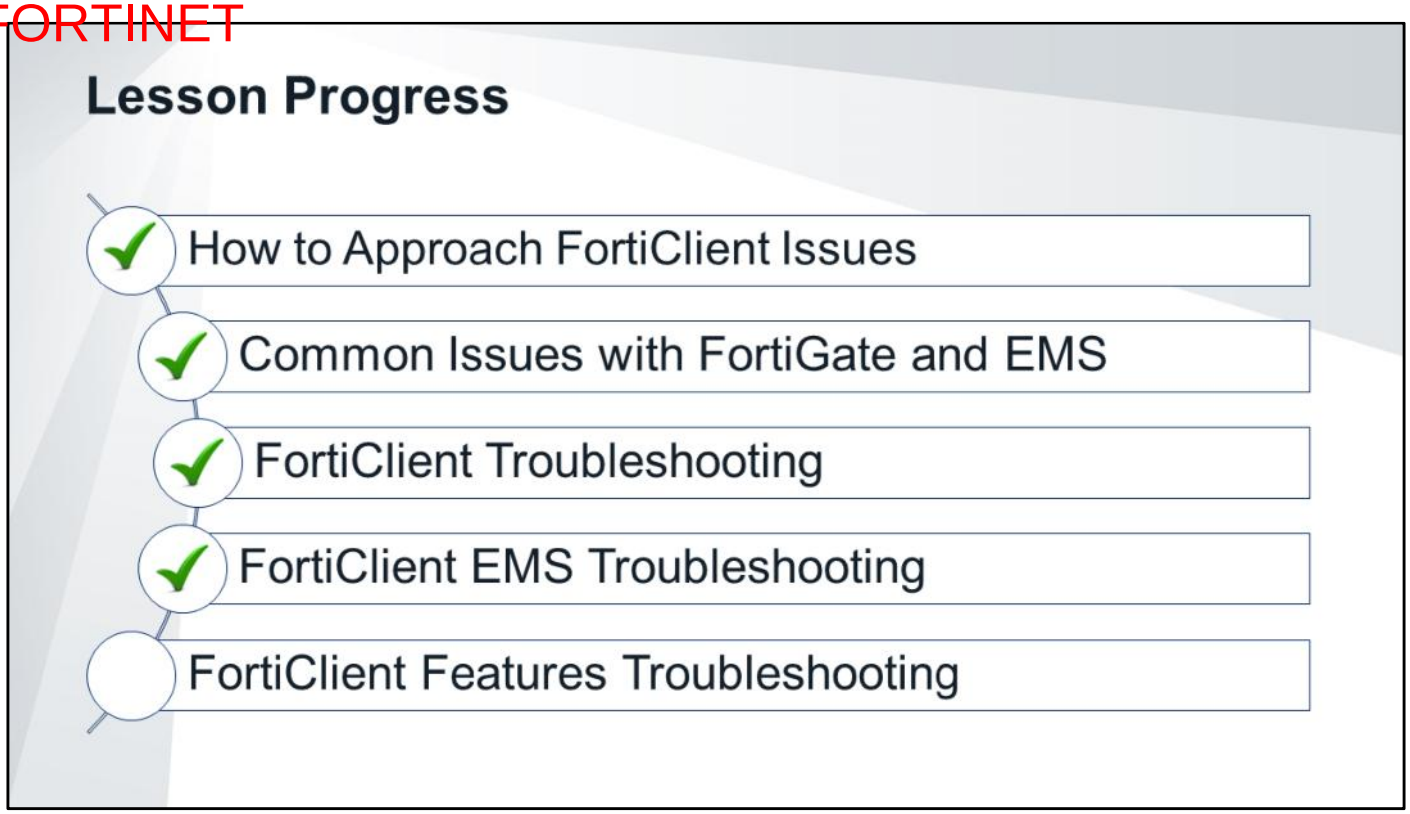
FORTINET

32

You can use the FortiClient EMS Diagnostic Tool to generate a debug report, and then provide the debug report to the FortiClient team to help with troubleshooting. For example, if you are working with customer support on a problem, you can generate a debug report, and send the report to customer support to help with troubleshooting.

The FortiClient EMS Diagnostic Tool does not record sensitive information. It contains information about the server that are shown in this slide.





Good job! You now understand FortiClient EMS components and troubleshooting on Windows Servers systems.

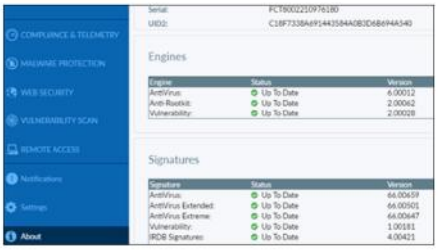
Now, you will learn about diagnosing and troubleshooting FortiClient features.

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in diagnosing FortiClient features, you will be able to resolve issues related to individual features.

FortiClient Features—Updates

- Verify latest updates
  - Click **About**
  - In an elevated command line window run the following
    - `update_task.exe -s fd_01`
- Registry
  - FA_UPDATE
  - FA_Scheduler\00003
- Check XML configuration
  - `<forticlient_configuration> <system> <update>`
  - Check custom servers if defined
    - Backup server
    - Failover to FDN
  - Schedule update




```
<update>
    <use_custom_server>0</use_custom_server>
    <restrict_services_to_regions />
    <server />
    <port>80</port>
    <timeout>60</timeout>
    <failoverport />
    <fail_over_to_fdn>1</fail_over_to_fdn>
    <use_proxy_when_fail_over_to_fdn>1</use_proxy_when_fail_over_to_fdn>
    <auto_patch>0</auto_patch>
    <submit_virus_info_to_fds>1</submit_virus_info_to_fds>
    <submit_vuln_info_to_fds>1</submit_vuln_info_to_fds>
    <update_action>notify_only</update_action>
    <scheduled_update>
        <enabled>1</enabled>
        <type>interval</type>
        <daily_at>01:09</daily_at>
        <update_interval_in_hours>1</update_interval_in_hours>
    </scheduled_update>
</update>
```

FORTINET

 36

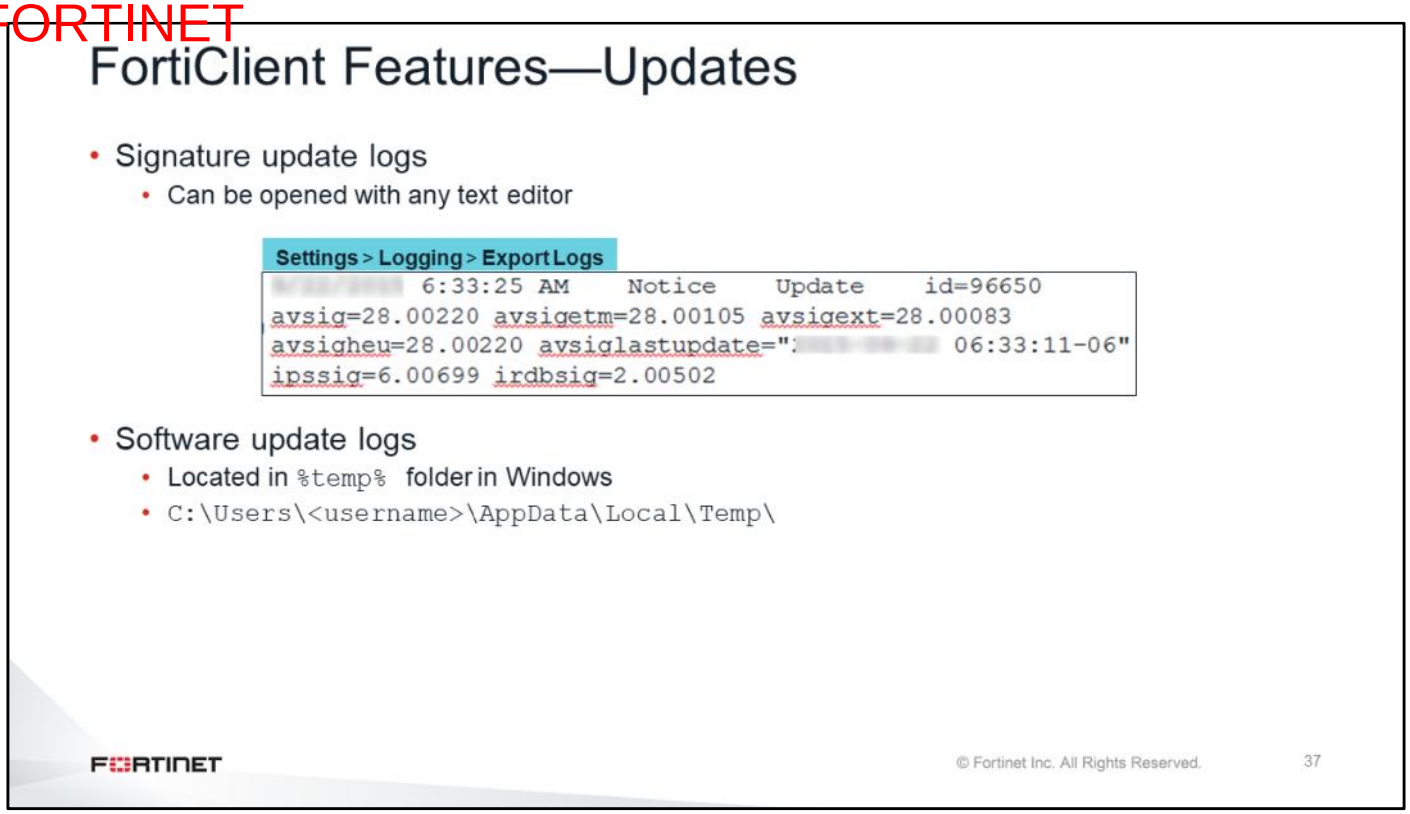
The FortiClient console provides the latest information about engine and software statuses and versions used by FortiClient. To check the latest updates on FortiClient, click **About**.

By default, the value for `use_custom_server` element is 0, which means it is disabled, failover backup servers are not defined, and failover to public FDN is enabled. In this case, FortiClient will first attempt to connect to the public FortiClient server, `forticlient.fortinet.net` or `myforticlient.fortinet.net`, over TCP port 80 to download the list of secondary servers from which it will then download the signatures and packages for FortiClient.

If a string is specified in `server` element and communication fails with that server, each of the servers specified in `fail_over_servers` element are tried until one succeeds. If that also fails, then software updates will not be possible unless `fail_over_to_fdn` is set to 1. If communication fails with the server(s) specified in both `server` and, `fail_over_servers` elements, `fail_over_to_fdn` specifies the next course of action.

You should leave the value of `fail_over_to_fdn` element to 1, which is the default value.

By default, scheduled updates are enabled at an intervals, these intervals specify the frequency that FortiClient checks for updates. A network error will cause an update failure, and the temporary AV signatures keep growing. Run the `update_task command` manually.



The signature update logs provide the date and time of the update, along with the version number of the signatures. You can export the logs to a local computer from FortiClient on **Export Logs** option. Based on the logging level and log types enabled, it will export all types of logs.

The software update logs are located in the `temp` folder in Windows, which might be a hidden folder.

FortiClient Features—Antivirus

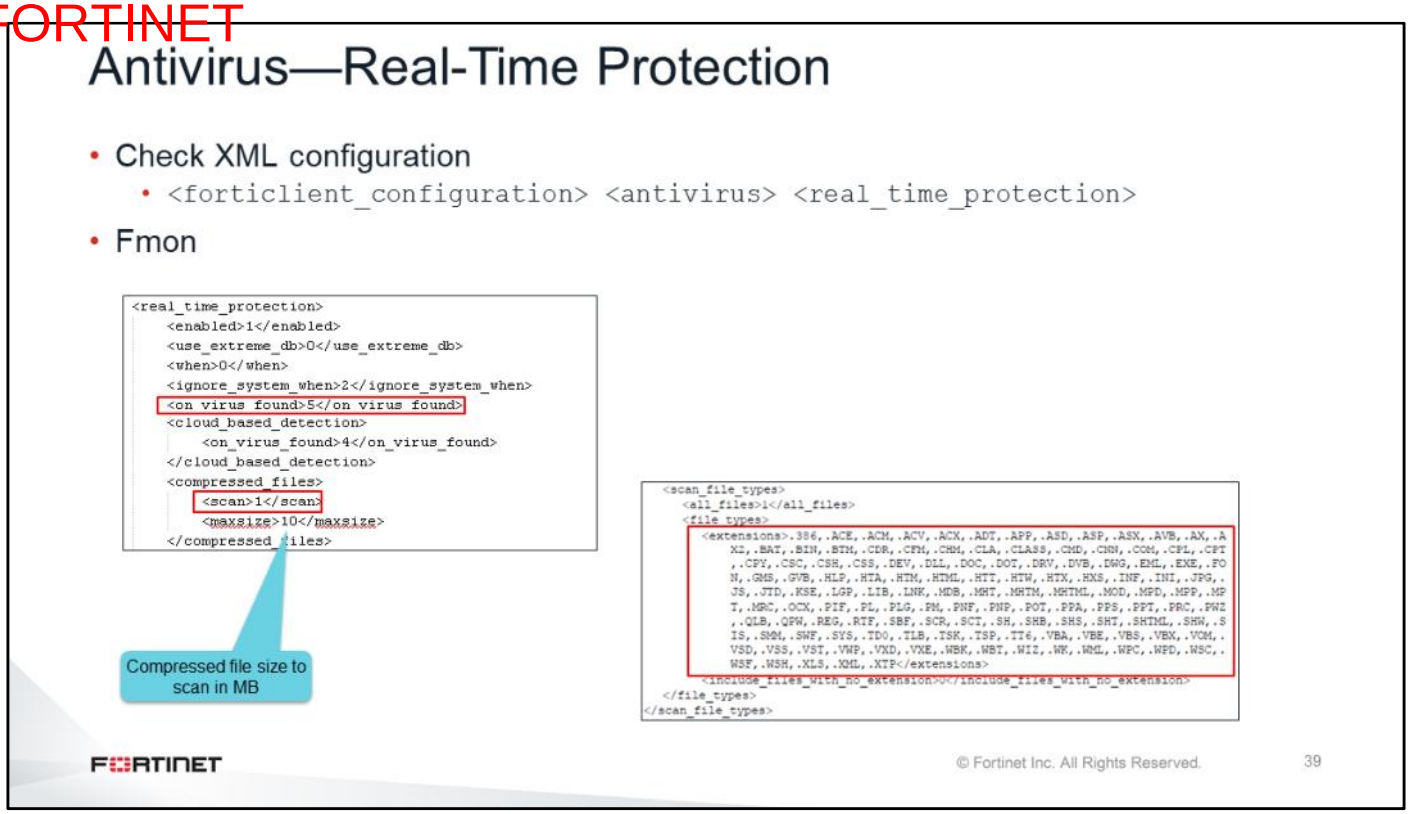
- Files and drivers:
  - fmon.exe, xmlav.dll, libav.dll, mdare.dll, mdare.sys
- vir_sig folder contains
  - Malware and antivirus signatures
    - Mdare_sig, vir_ext, vir_extreme, vir_heuristics, vir_high, vir_high
  - fdni.conf—list of FortiGuard severs
  - Block malicious websites
    - fortiwf.exe, fortiwf2.sys
  - Block known communication channels
    - fortifws.exe, fortisniff.sys, irdb.dat

```
SerialNumber=FPT-FCS-29500013|Address=208.91.112.135:443|FDNListener=208.91.112.135:8889|TimeZone=-5
SerialNumber=FPT-FCS-DELL0005|Address=208.91.112.132:443|FDNListener=208.91.112.132:8889|TimeZone=-5
SerialNumber=FPT-FCS-DELL0008|Address=208.91.112.133:443|FDNListener=208.91.112.133:8889|TimeZone=-5
SerialNumber=FPT-FCS-DELL0015|Address=208.91.112.136:443|FDNListener=208.91.112.136:8889|TimeZone=8
```

FORTINET

38

FortiClient requires a number of files and drivers in order to perform a real-time antivirus scan which includes EXE, DLL, SYS, and CONF files, and are located in `Installation directory\Fortinet\FortiClient\` folder. The `vir_sig` folder contains malware and antivirus signatures along with the `fdni.conf` file, which contains a list of public FortiGuard servers that FortiClient contacts to get updates on the signatures and packages.



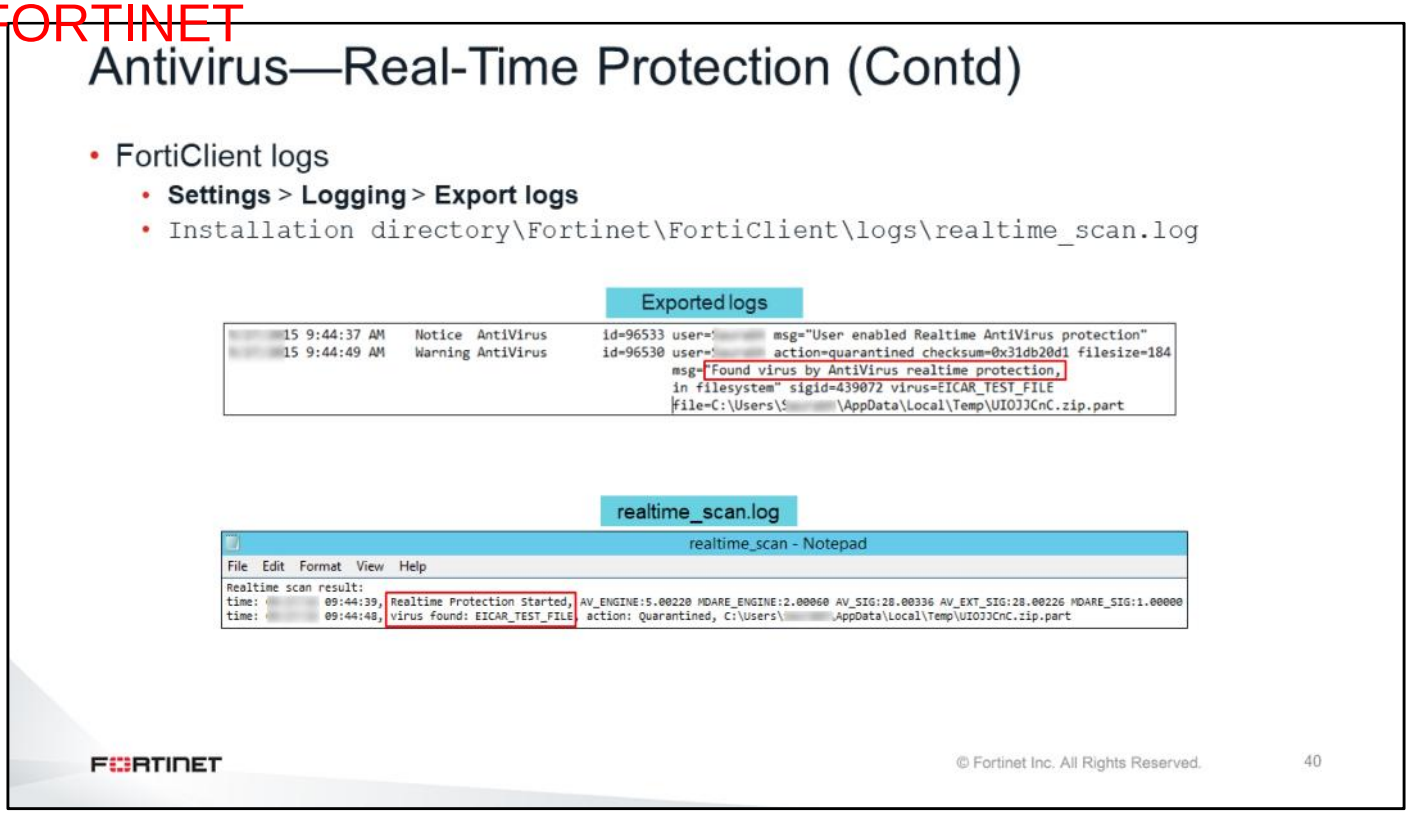
It is very important to check the XML configuration if the real-time antivirus protection is not functioning properly. By default, when a virus is found, FortiClient block access to the file. There are five levels of `on_virus_found` XML configuration tags:

- 0: clean
- 1: ignore
- 2: repair
- 3: warning
- 4: quarantine
- 5: deny access

FortiClient also performs a scan on the compressed files and allows you to define the compressed file size to scan up to 65535MB. 0 means no limit. FortiClient performs a real-time scan on a wide range of extensions and allows you to modify the list of extensions to scan.

For example, if you set the value of the `on_virus_found` XML configuration tag to 1, it will ignore the virus file and the virus will not be caught. Another example is if you modify and remove a few extensions from the `extensions` XML configuration element and if the suspicious file extension is not listed in the `extensions` XML configuration element, it will not be caught.

Note that this partial XML configuration is for a real-time antivirus. For a complete list of available XML configuration elements, refer to the *FortiClient 6.2.0 XML Reference guide* available at Fortinet documentation site.

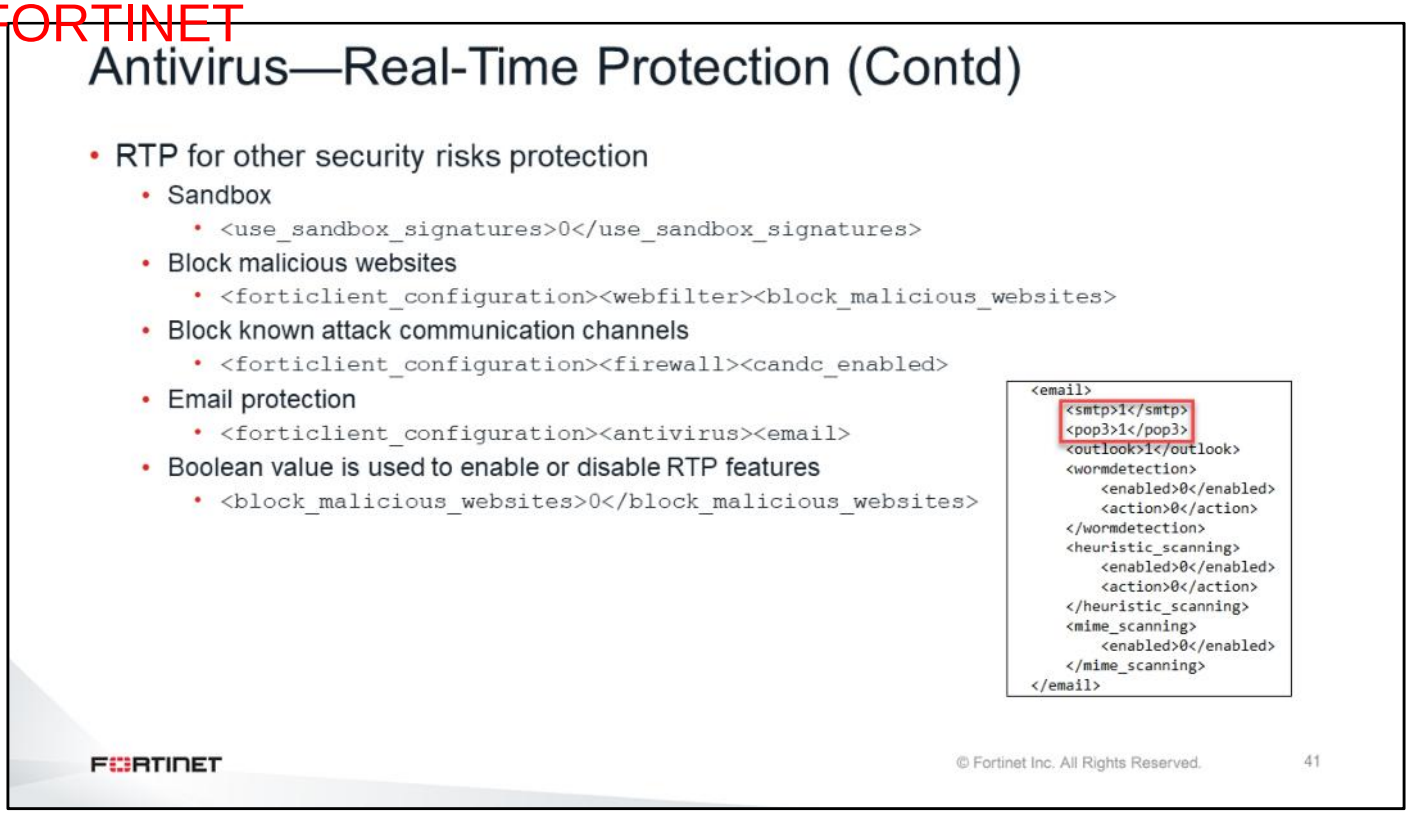


The antivirus logs provides the date and time of the real-time antivirus scan along with the action taken, virus, and location of the file. To export the logs to a local computer from FortiClient, select **Settings** > **Logging** > **Export Logs** option.

Based on the logging level and log types enabled, **Export Logs** will export all types of logs.

The `realtime_scan.log` located in `Installation directory\Fortinet\FortiClient\logs\realtime_scan.log` provides more detailed information about malware and antivirus engines and signatures used in the real-time antivirus scan, along with name of the virus file, action taken, and location of the file.

Debug: In an elevated command line window:
- Disable RTP on FortiClient.
- Change the FortiClient installation directory: `fmon.exe -s -fd_1`



There are other security risks that are also handled by real-time protection. The sandbox signatures can also be used by FortiClient to identify the threat. Block access to malicious websites function blocks malicious websites. The web filter module must be installed before you can enable this protection.

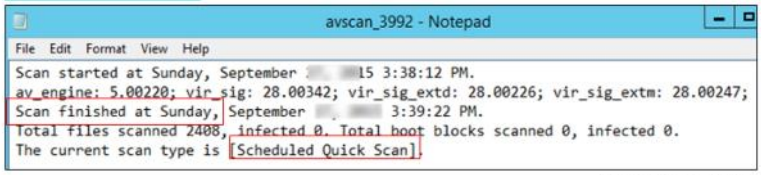
FortiClient RTP also block known communication channels used by attackers. The application firewall module must be installed before you can enable this protection. An Email protection on FortiClient scans email for malicious files. It supports POP3 and SMTP.

You can use Boolean values in EMS XML editor to enable or disable real-time protection features. The booleon value 0 for `<block_malicious_websites>` in this slide will disable blocking of malicious websites.

Antivirus—Schedule and Custom Scan

- Uses the same files and drivers as real-time antivirus scan
  - Uses `av_task.exe` instead of `fmon.exe`
  - `av_task.exe <options>`
    - `-q` - quick scan
    - `-f` - full system scan
    - `-d <dir>` - scan the specified directory
    - `-x` - use multiple `av_task.exe` instances for scanning
- Check XML configuration
- `<forticlient_configuration> <antivirus> <scheduled_scan>`
- `<forticlient_configuration> <antivirus> <on_demand_scannning>`
- FortiClient Logs

avscan_xxxx.log



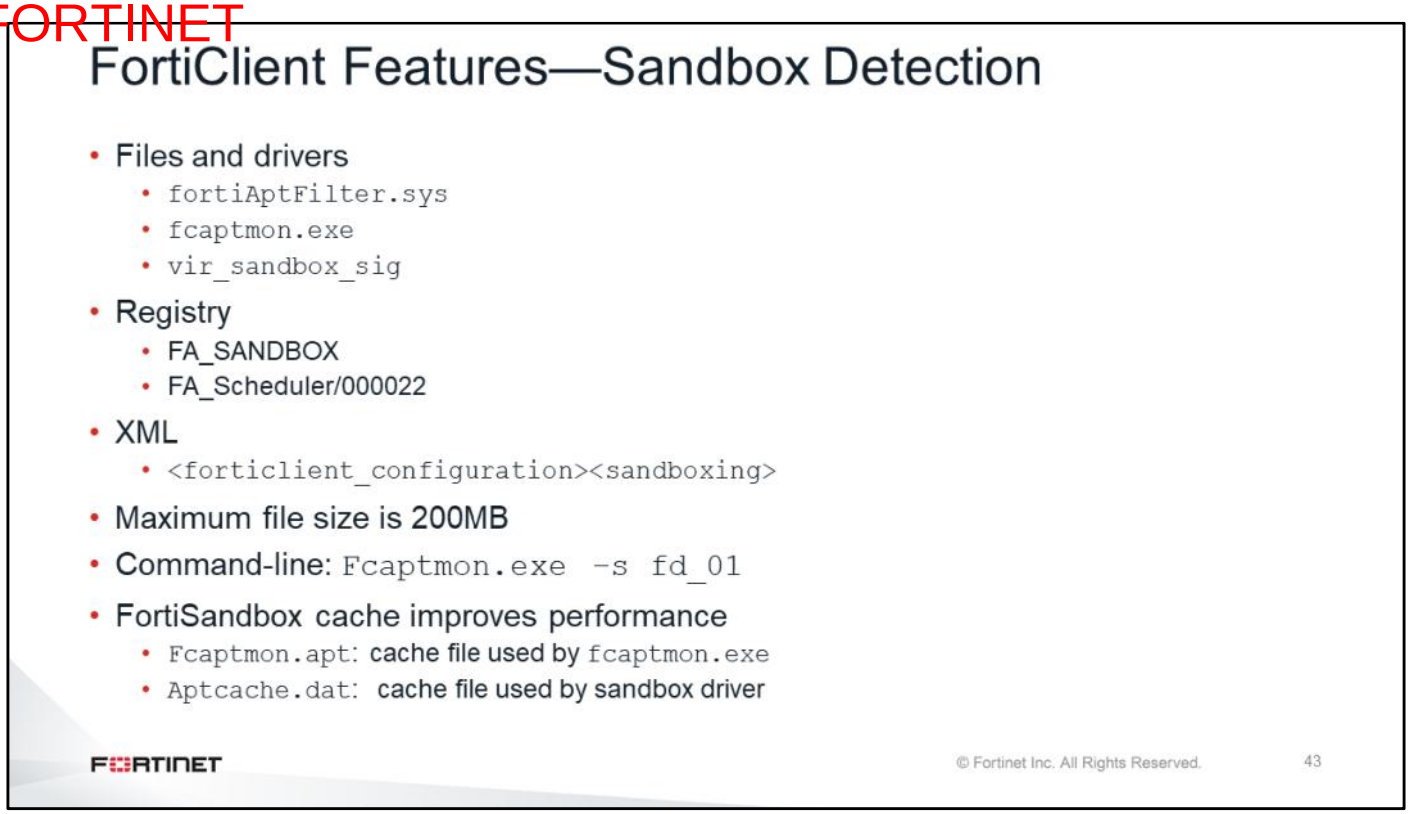
FORTINET

42

The scheduled and custom scan uses the same real-time antivirus files and drivers except it uses `av_task.exe` instead of `fmon.exe`. It uses `av_task.exe` file with option `-f` to perform a full system scan and `av_task.exe -d` to scan the specified directory.

The factory default behaviour at the time of installation is to run a full system scan on the first day of the month at 18:30 hours and it also scans removable media. However, default XML configuration file can be modified to change the default behaviour. You can view and modified factory default full scan schedule under full element of the XML file.

There is a priority parameter in the XML file as well. By default, the priority of the scan is set to normal and has three different levels–0 for normal priority, 1 for low priority and 2 for high priority. The `on_demand_scanning` element defines how the antivirus scanner handles the scanning of files manually requested by the end user. The scheduled and on-demand scan logs are located in `Installationdirectory\Fortinet\FortiClient\logs\av_scanxxxx.log`.

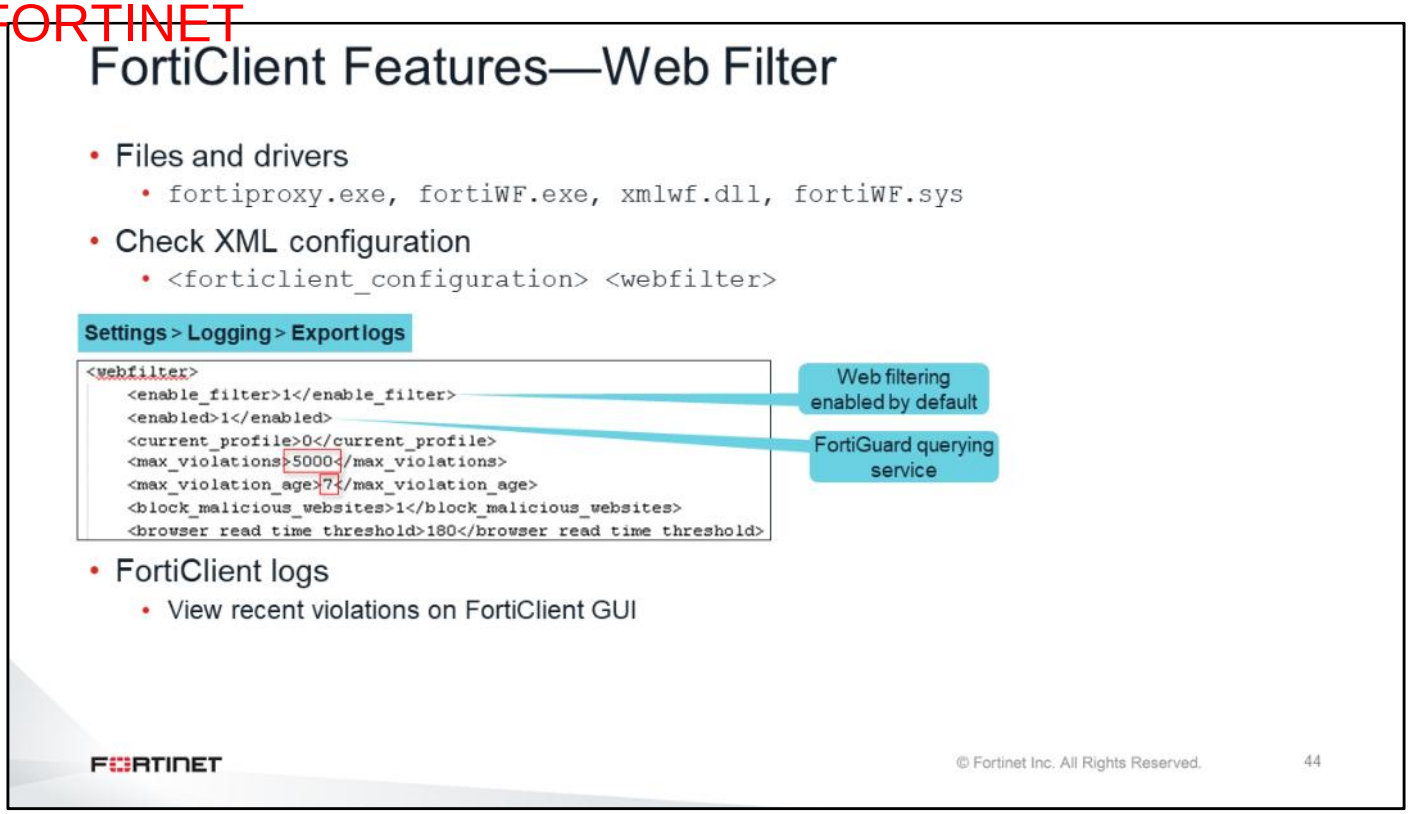


FortiClient requires a number of files and drivers in order to perform file submission to FortiSandbox. The `vir_sanbox_sig` folder contains malware and antivirus software. The maximum file size you can submit from FortiClient to FortiSandbox is 200MB.

Files can be submitted from the following sources:
- Removable media
- Mapped network drives
- Web downloads
- Email download

You can run a sandbox debug by entering the CLI command `Fcaptmon.exe -s fd_01` in an elevated command-line window.

FortiSandbox also caches files to improve performance.



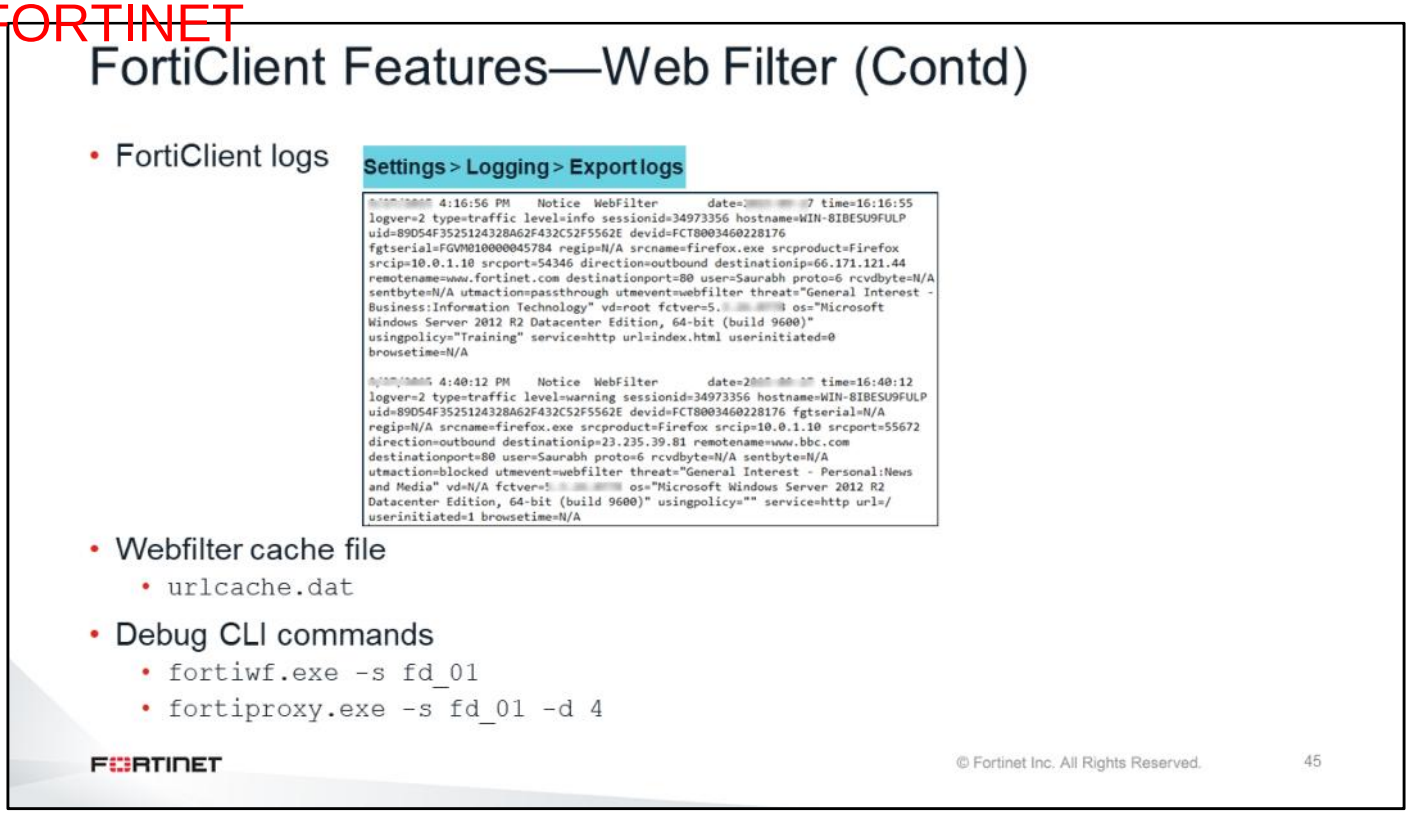
FortiClient requires a number of files and drivers in order to perform web filtering. By default, web filtering and the FortiGuard querying service are enabled, and can store up to 5000 violations for a period of seven days. The default value for `max_violations` element is set to 5000 and can be ranged from 250 to 5000, and `max_violation_age` element is set to seven days and can be ranged from 1 to 90 days.

You can also configure safe search and the YouTube education filter under the `<safe_search>` and `<youtube_education_filter>` XML elements.
For a complete list of available XML configuration elements, refer to the *FortiClient 6.2.0 XML Reference guide* available at `http://docs.fortinet.com`.

Safe Search is a feature of Google search that acts as an automated filter of pornography and potentially offensive content. The upcoming release of FortiClient will include the ability to modify the host file to force all Google or YouTube traffic to connect to safe search websites, such as WackySafe, that only delivers safe search results. The drawback is that this will affect all Google services, such as search, YouTube, and so on.

Enabling the Client Web Filtering When On-Net option will keep using the FortiClient web filter even if it is behind FortiGate and on-net. When this is disabled, FortiClient endpoint will be protected by FortiGate web filter profile when on-net.

You can view the web filtering violation logs directly on the FortiClient GUI or export the logs from **Export Logs**.

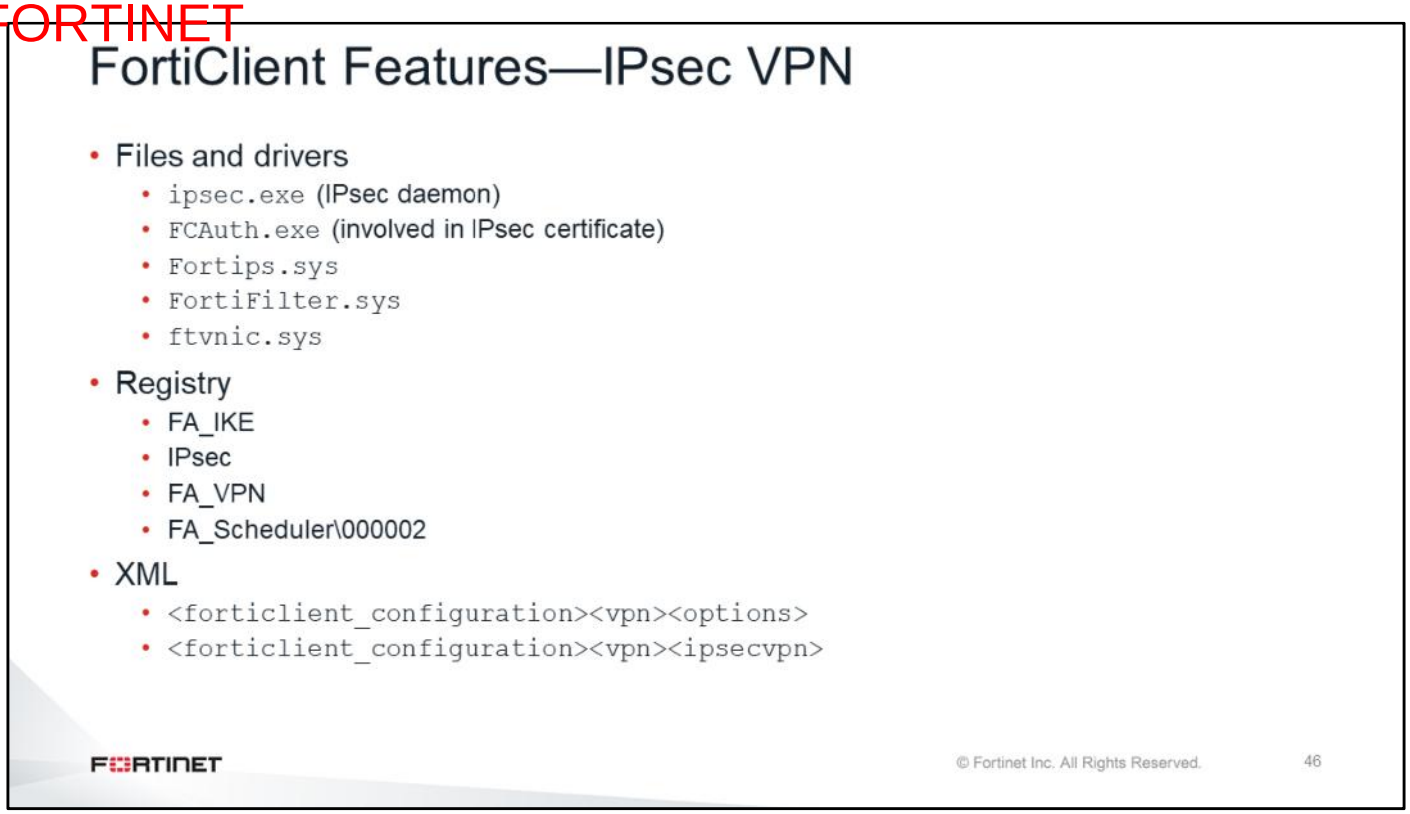


In the example shown on this slide, the first log entry is from a FortiClient that is managed by EMS and FortiGate (integrated mode). The managed FortiClient log show the FortiGate serial number along with the name of the FortiClient profile it is using, and other details such as utmaction, utmevent, and so on.

So, when diagnosing and troubleshooting web filtering issues, always pay attention to the logs because the URL or category might be blocked in the managed profile, but allowed in the URL list, and the results might be different than what you were expecting.

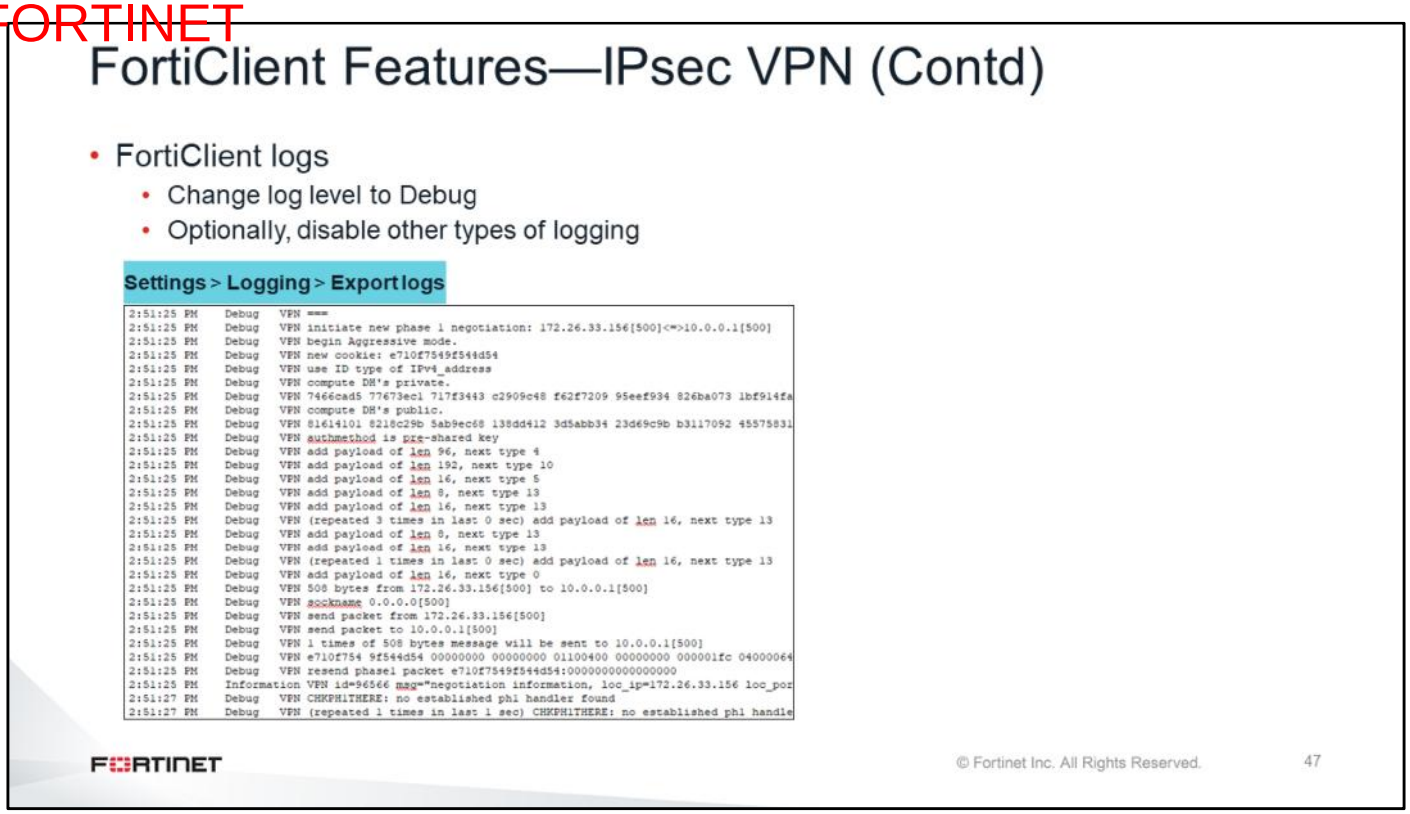
- The webfilter cache URL rating results in the `urlcache.dat` file. You can also run the CLI commands `fortiwf.exe -s fd_01` and `fortiproxy.exe -s fd_01 -d 4` in elevated mode, to further troubleshoot webfilter issues:

The above commands provide debug level logs for web filter and FortiProxy processes.



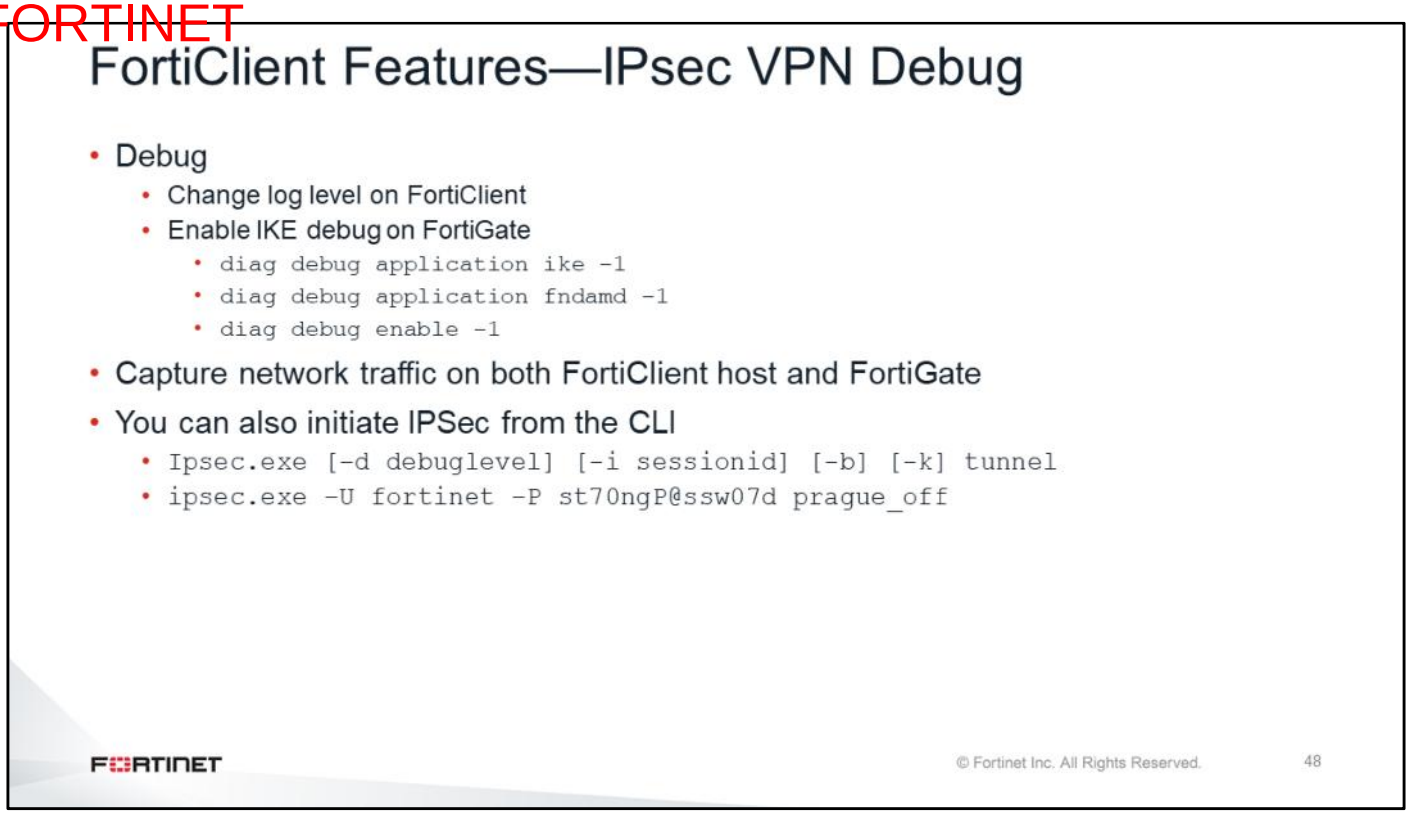
FortiClient requires a number of files and drivers for IPsec VPN.
The VPN-related information is contained inside the `VPN>` XML tags. The `options` XML tag contains global options that apply to both SSL VPN and IPsec VPN as shown in this slide.

The `ipsecvpn` XML tag contains configurations specifically related to IPsec VPN.
IPsec VPN has two subsections:
- Options: Options related to the specific type of VPN
- Connections: User-defined connections



VPN-related logs can be exported from **Export logs**. When troubleshooting VPN issues, as a best practice, change the log level to `Debug` and disable other types of logging to minimize the logs from other features.

The FortiClient-FortiGate dialup request is sent from FortiClient towards FortiGate. FortiClient-FortiGate negotiates using aggressive mode. In aggressive mode, the IKE SA contains almost everything, such as the encryption type, length, hash type, and Diffie–Hellman (DH) group. It contains fewer exchanges and packets and is faster than main mode.

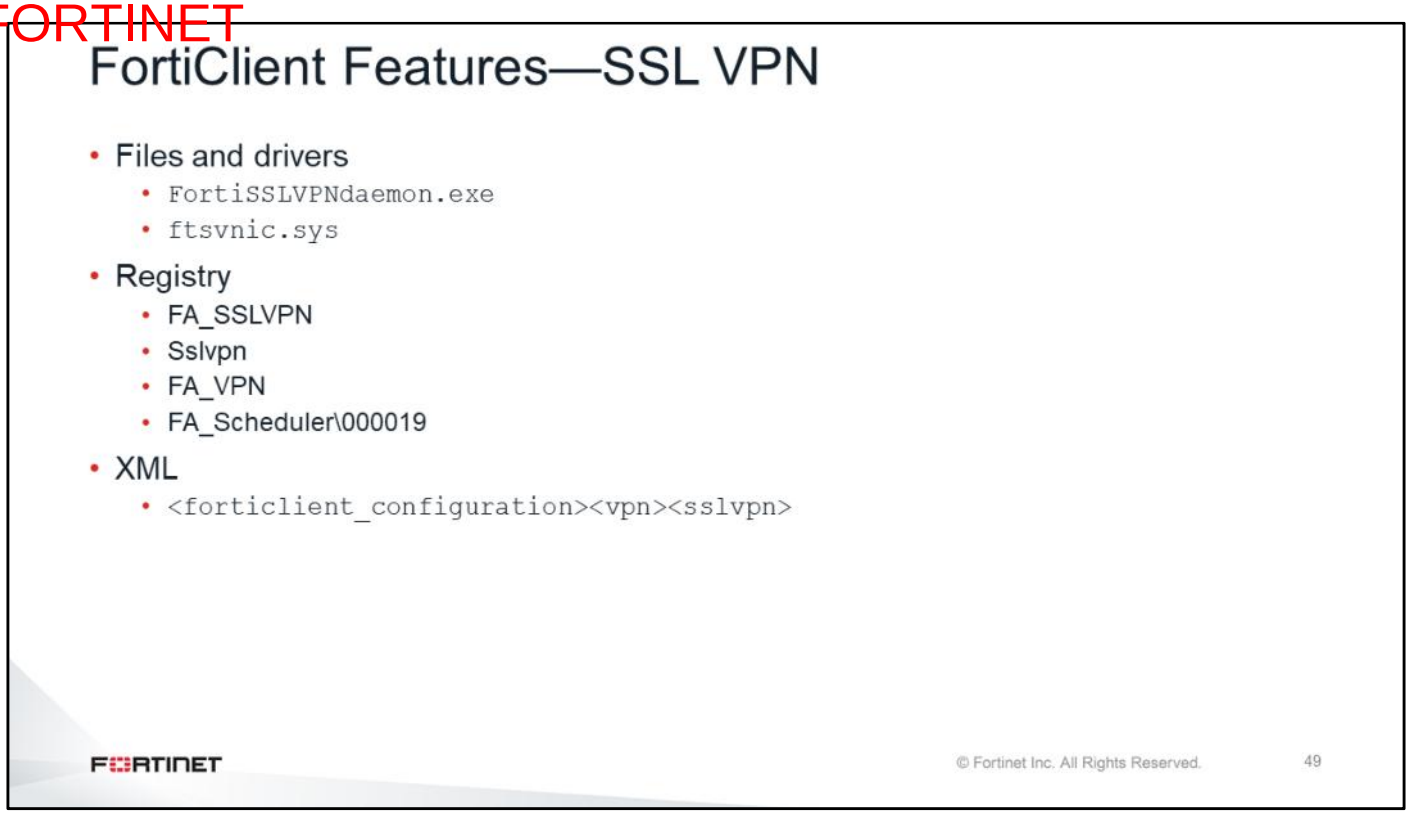


You can run the real-time debug commands on FortiGate, which will show you the similar information as on FortiClient.

As a best practice, run the debug commands on FortiGate to compare with the IPsec VPN logs on FortiClient.

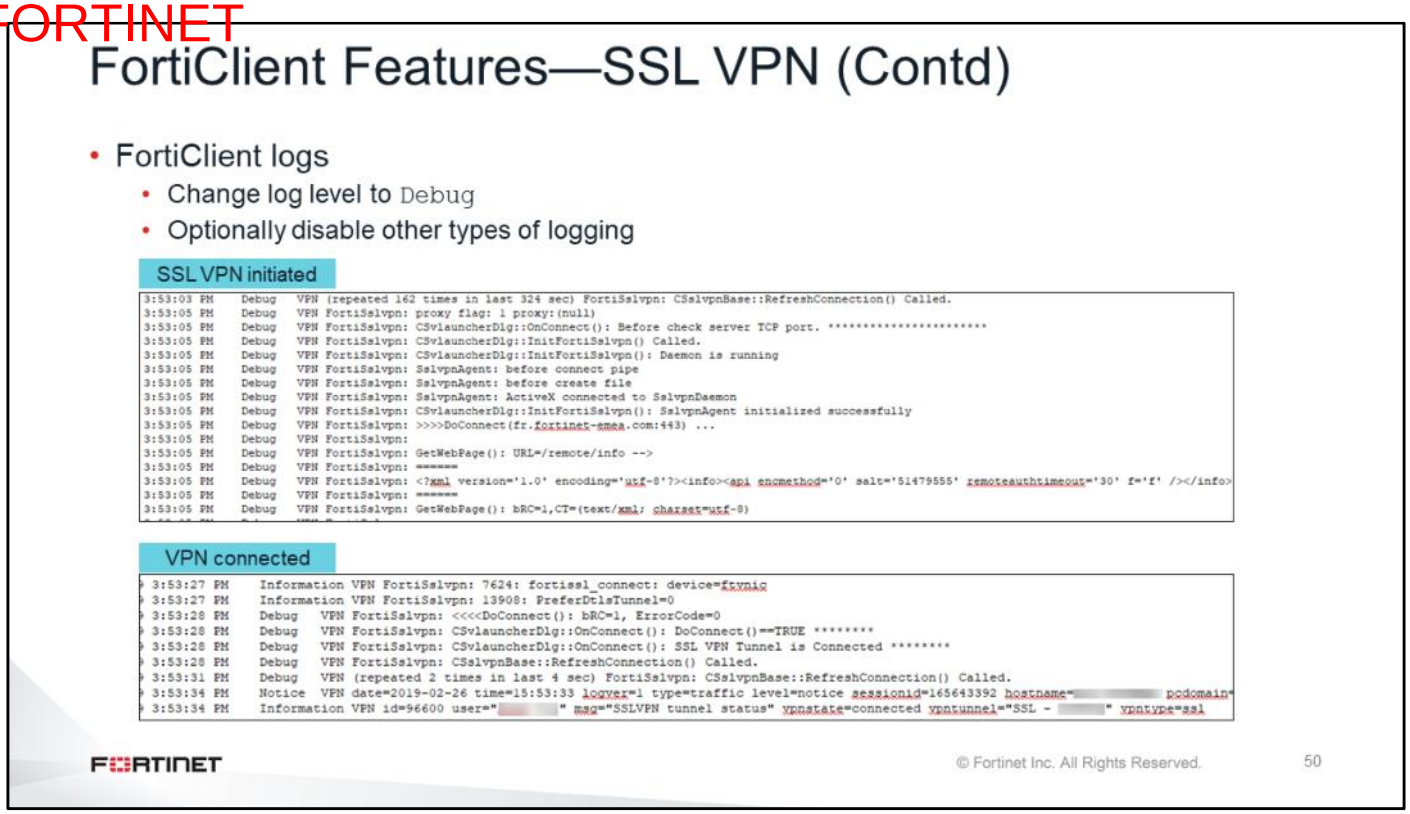
Apart from the real-time debug command shown on the slide, you can also run the following commands on FortiGate device to troubleshoot IPsec VPN issues:

- `diagnose vpn ike config list` command checks the configuration as it is seen by IKE daemon on the FortiGate device
- To list IKE SA on the FortiGate device, run `diagnose vpn ike gateway list`
- To list IPsec SA on the FortiGate device, run `diagnose vpn tunnel list`
- To check status of all tunnels (equivalent to GUI VPN monitor) on the FortiGate device, run `get ipsec tunnel list`
- To check routes on the FortiGate device that were installed by the IKE daemon (applicable only for dialup IPsec VPN), run `diagnose vpn ike routes list`



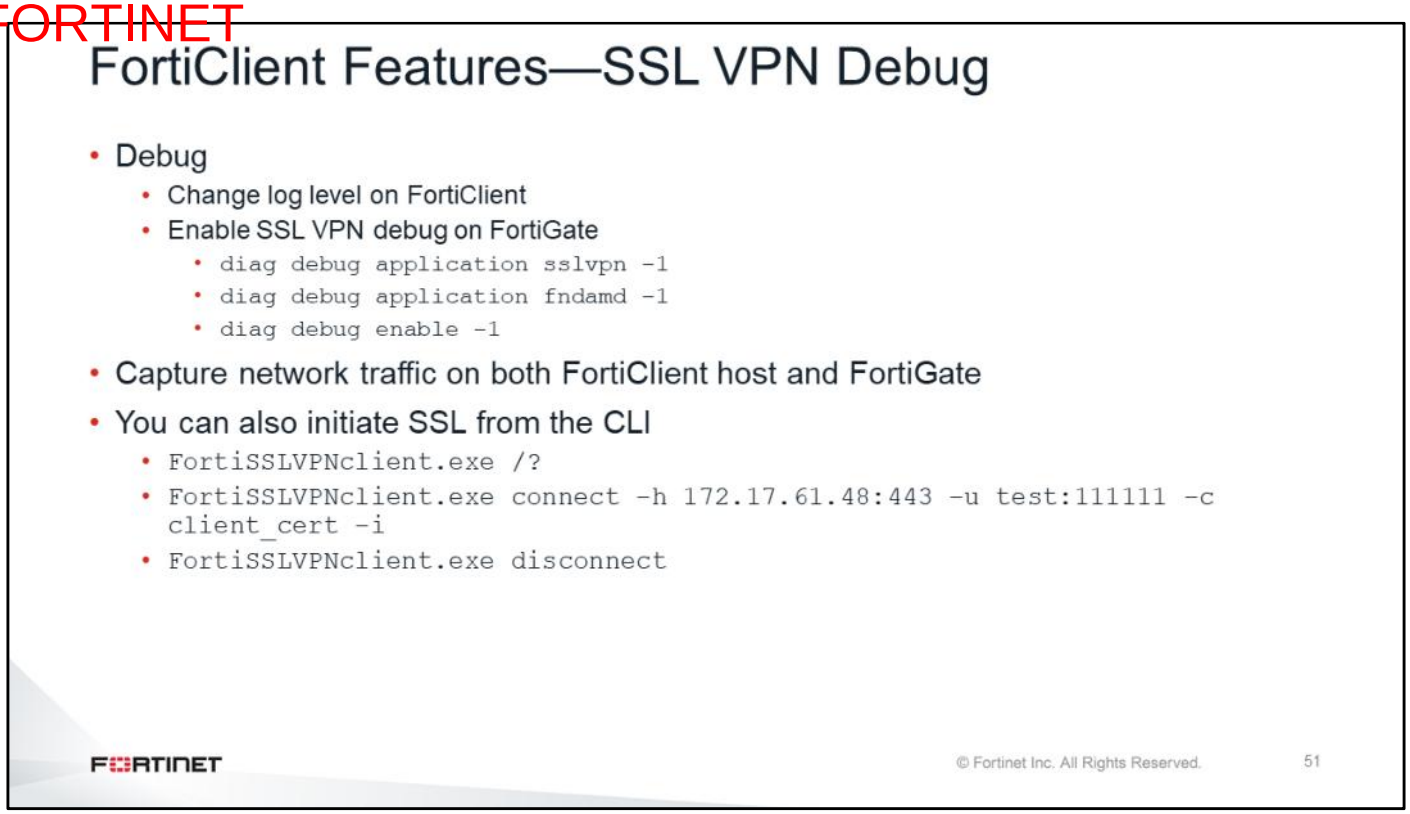
The FortiClient requires a number of files and drivers for SSL VPN.

The `sslvpn` XML tag contains configurations specifically related to SSL VPN.
SSL VPN has two subsections:
- Options: Options related to the specific type of VPN
- Connections: User-defined connections



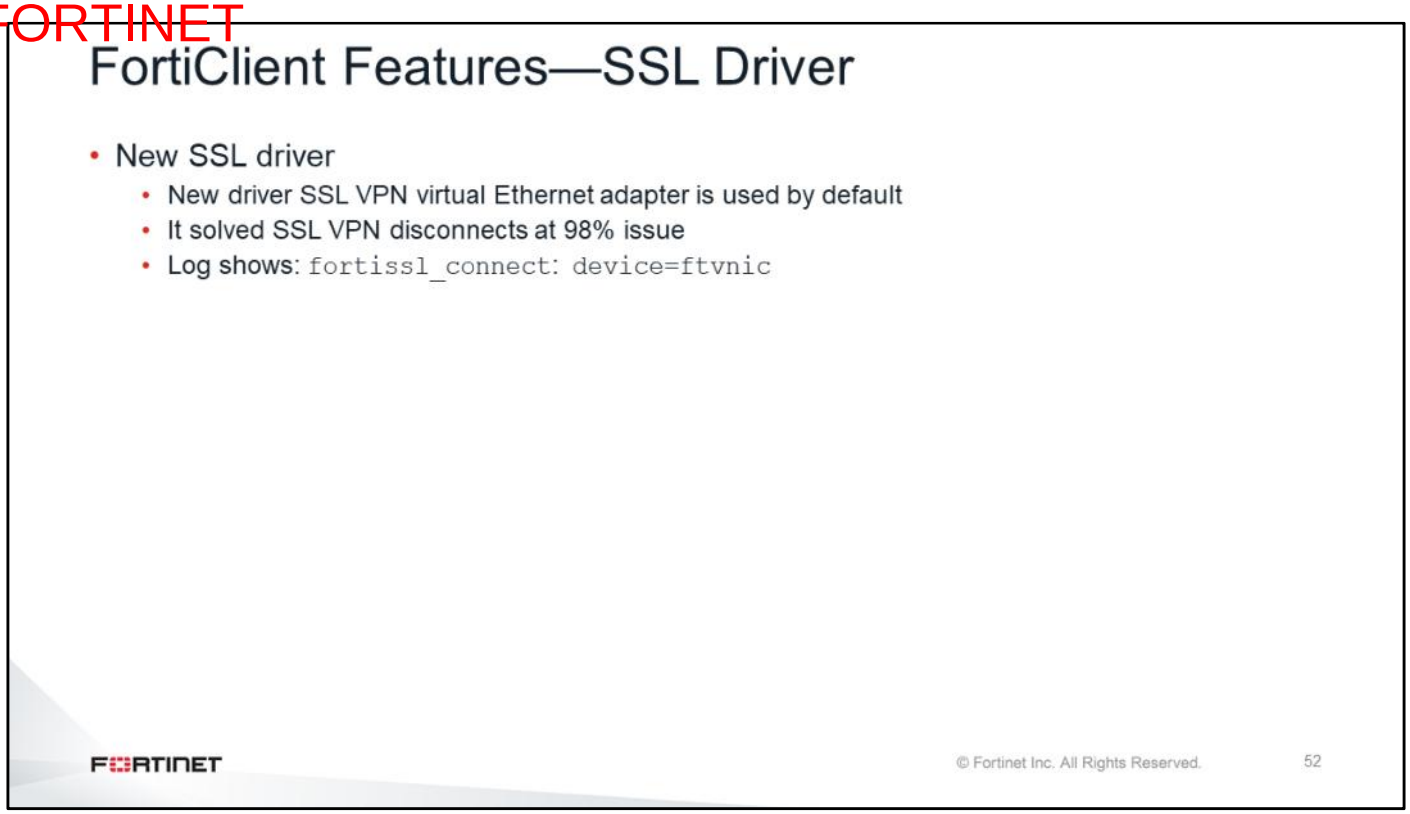
You can export VPN-related logs from **Export logs** pane of FortiClient. When troubleshooting VPN issues, as a best practice change the log level to `Debug` and disable other types of logging to minimize the logs from other features.

The FortiClient-FortiGate SSL VPN request is sent from FortiClient towards FortiGate. FortiClient-FortiGate checks the port number for the SSL VPN service and user credentials to allow access. The SSL debug logs show the initial connection requested made by FortiClient to FortiGate. Then the SSL certificate negotiation takes place between FortiClient and FortiGate. The FortiClient side certificate information is located in the `Installation directory\Fortinet\FortiClient` folder.

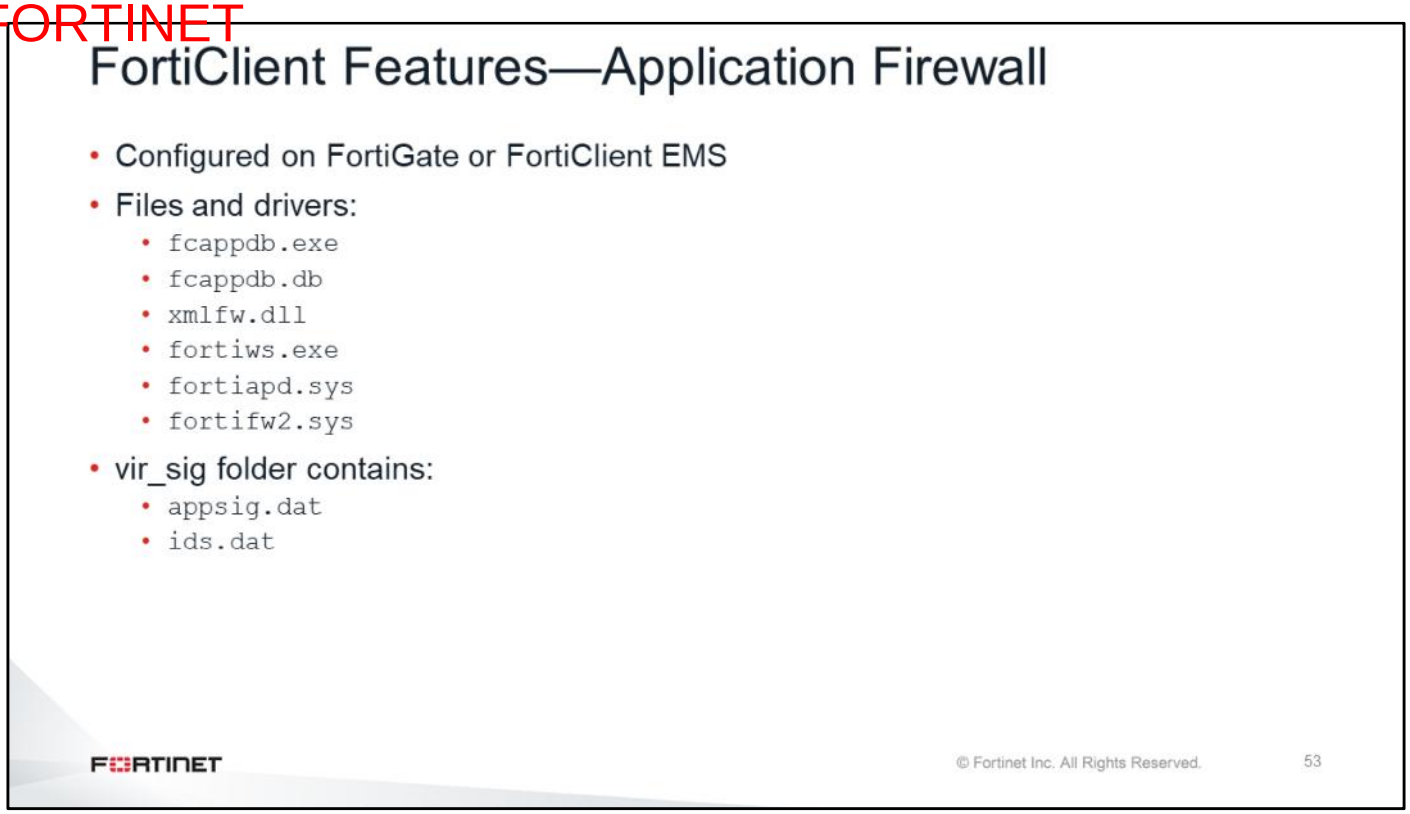


You can run real-time debug commands on FortiGate, which will show you the information that is similar to the information shown on FortiClient.

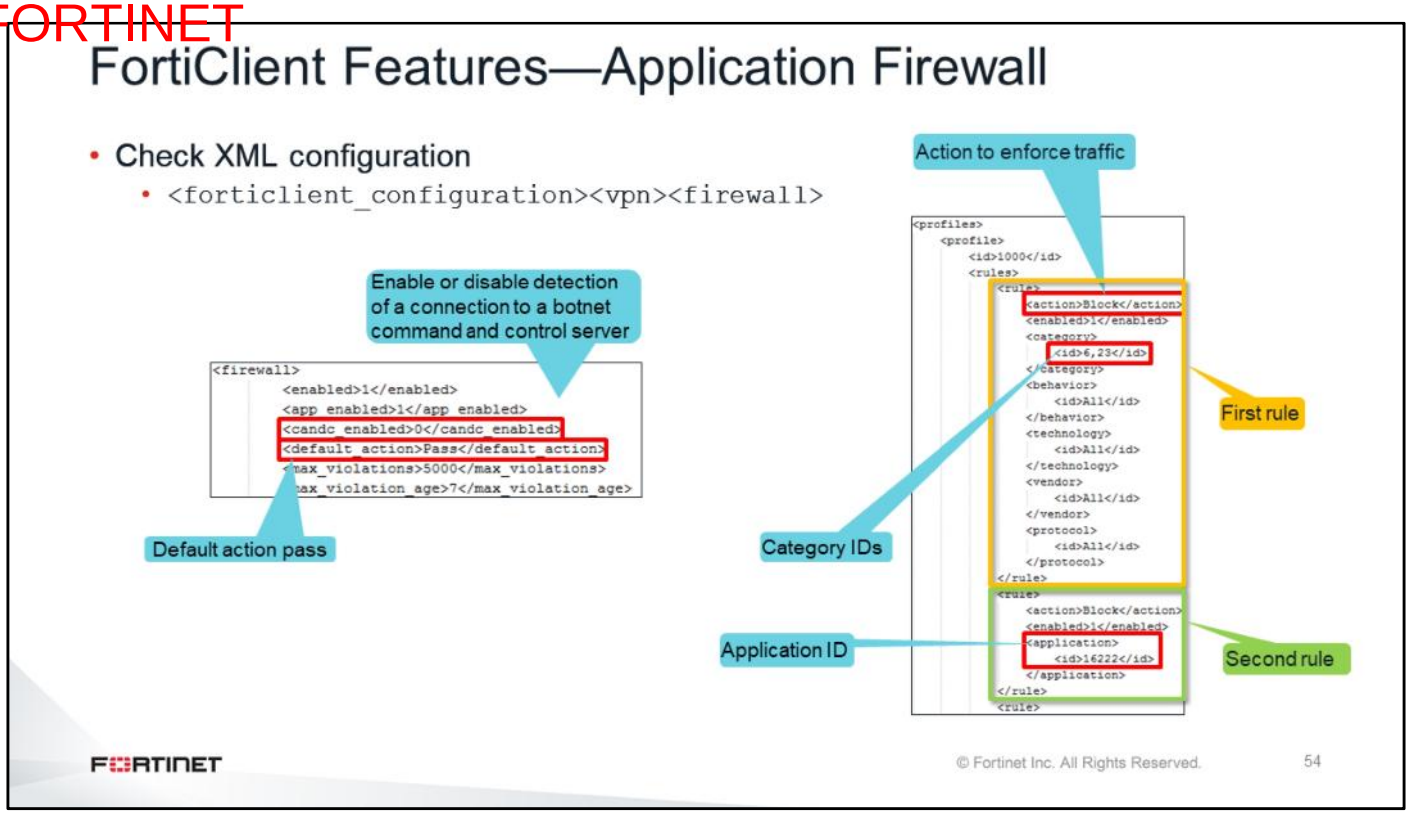
As a best practice, run the debug commands on FortiGate to compare them with the SSL VPN logs on FortiClient.



Fortinet added its own SSL driver, or virtual adapter, to resolve issues related to the Windows PPP Wan Miniport Adapter. By default, FortiClient uses a new SSL driver. In logs, it is shown as in this slide.



An application firewall uses an IPS engine, so it matches the patterns in the entire byte stream of the packet and requires multiple files and drivers.

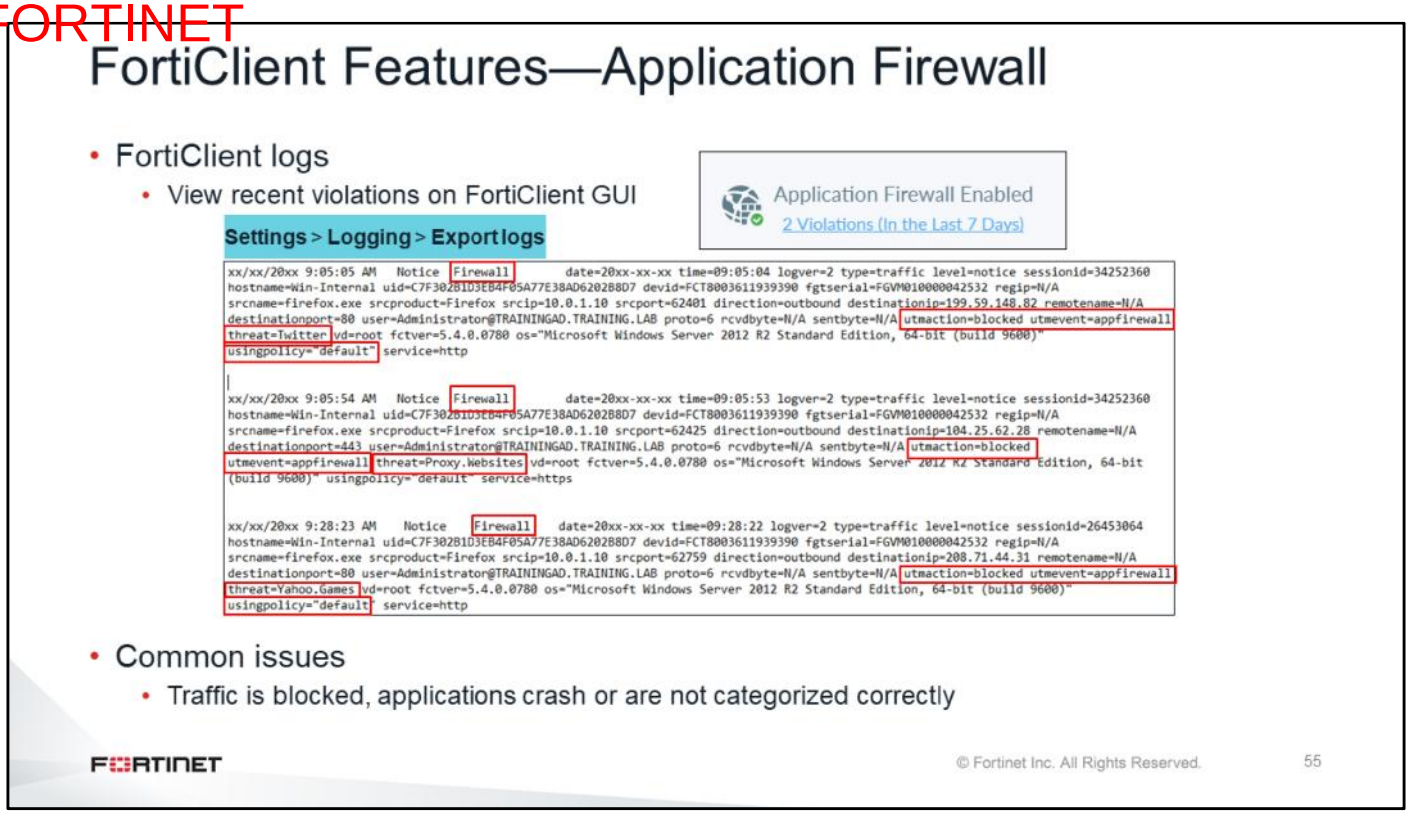


The application firewall XML configuration elements can be grouped into two parts, general options and profiles. A general option applies to all firewall activities and profile defines the applications and the actions that apply to the firewall activities.

You can enable the `candc_enabled` XML configuration element by setting the value equal to 1, to detect a connection to a botnet command and control server. The `default_action` XML configuration element value is set to `pass`, which enforces the action to pass on traffic that doesn't match any defined profiles. You can change the default action to `block`, `reset`, or `pass`. The `profiles` tag has a `rules` element. The `rules` element may, itself, have zero or more `rule` tags.
The following filter elements can be used to define applications in a `rule` tag:

- `category`
- `vendor`
- `behavior`
- `technology`
- `protocol`
- `application`
- `popularity`

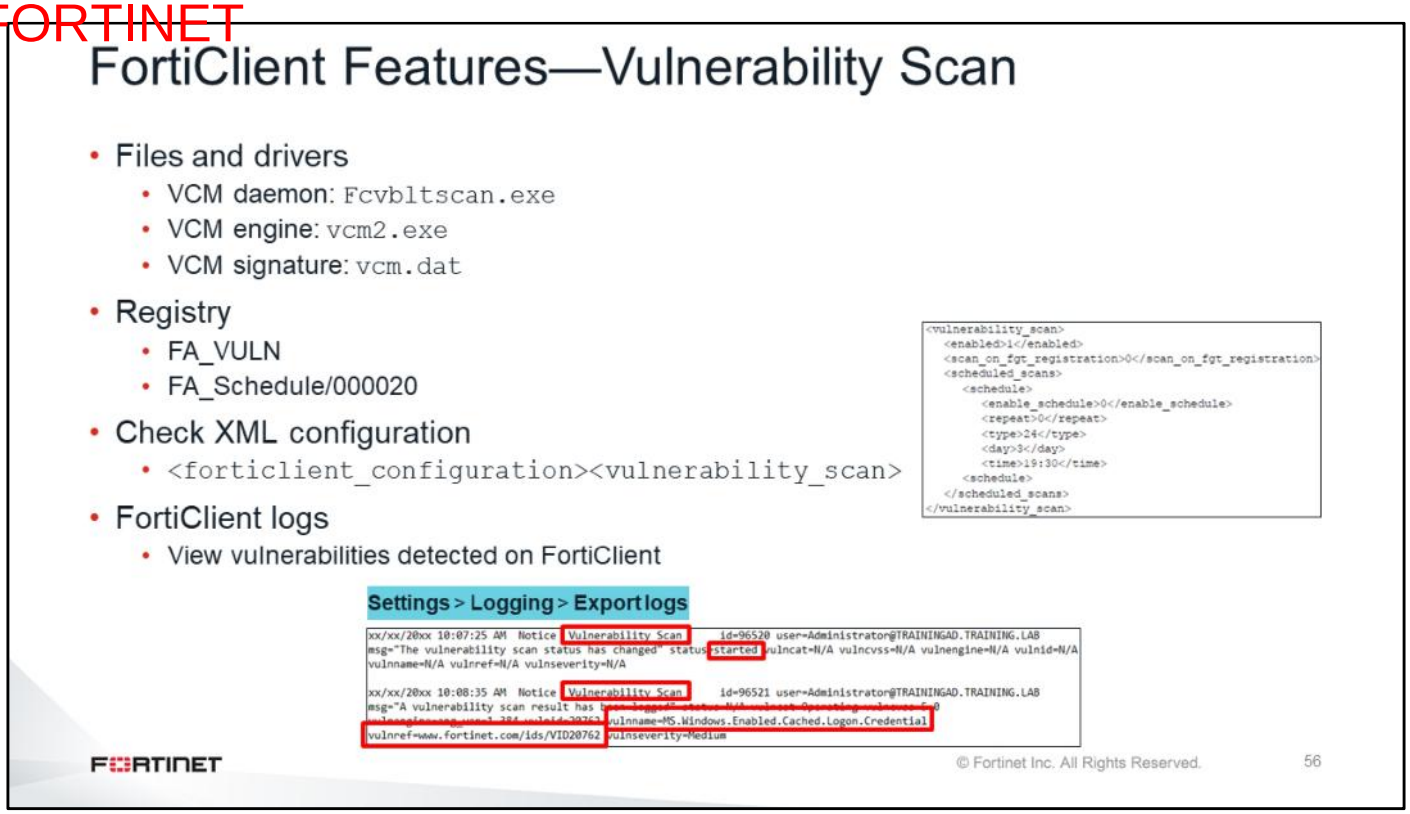
If the `application` element is present, all other sibling elements (listed above) will be ignored. If it is not present, a given application must match all of the provided filters to trigger the rule.
In the example shown on this slide, in the first rule, categories 6 and 23 are blocked, which corresponds to `Proxy` and `Social.Media` respectively. In the second rule, application 16779 is blocked, which is `Yahoo.Games`. You can get the complete list of IDs corresponding to each category, behaviour, and application from the FortiGate CLI.



You can view the application violation logs directly on the FortiClient GUI or export logs from **Export logs** option.

In the example shown on this slide, FortiClient blocks two categories (`proxy` and `Social.Media`) and the application `Yahoo.Games`, when FortiClient inspects the traffic passing through it and, based on the matching rule, takes action. In this example, FortiClient blocks Twitter, proxy websites, and `Yahoo.Games`, based on the defined rule.

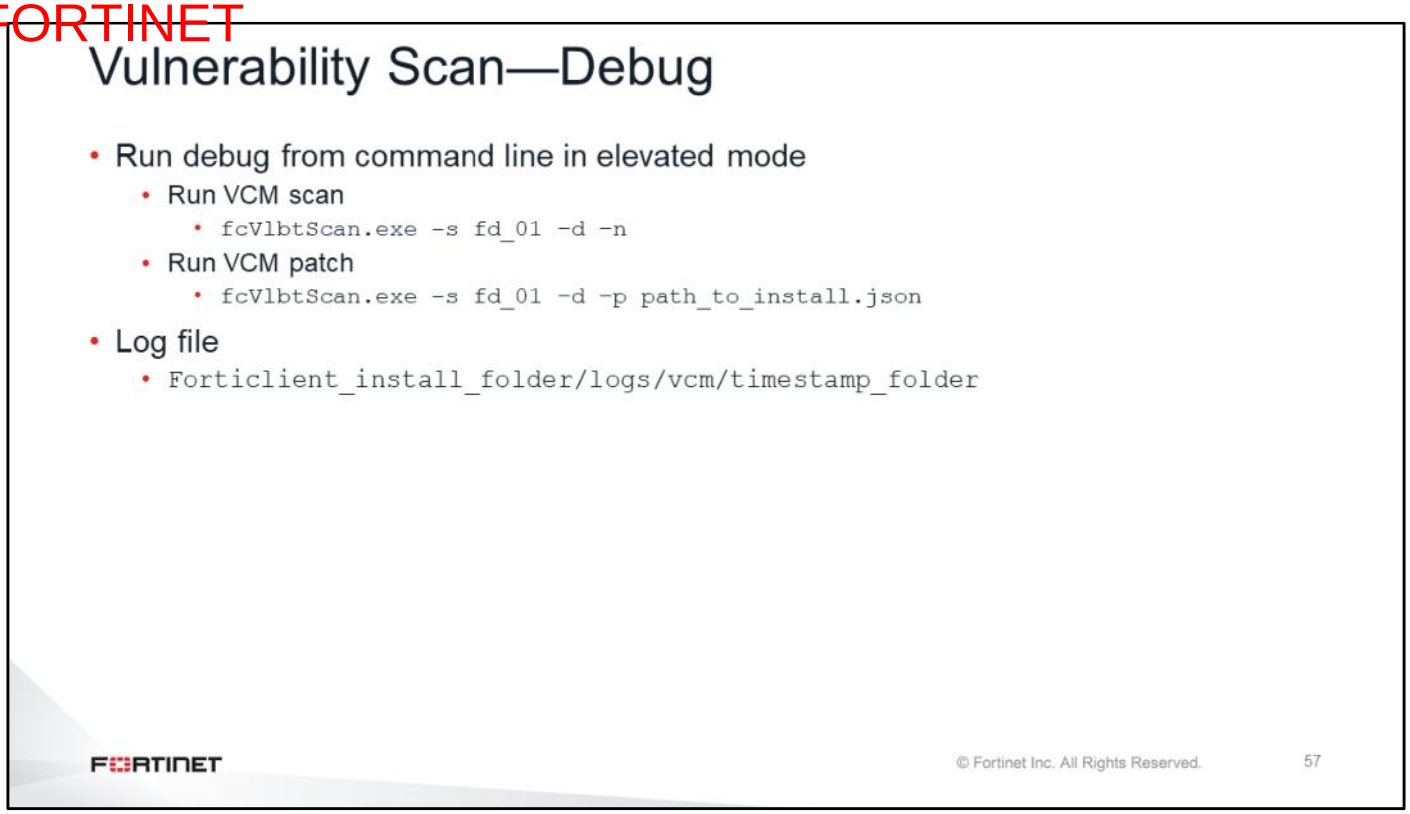
Some common issues are blocked traffic, and applications that crash, or are not categorized correctly.Try to disable FortiClient features one-by-one, to make sure the issue is caused by the application firewall.



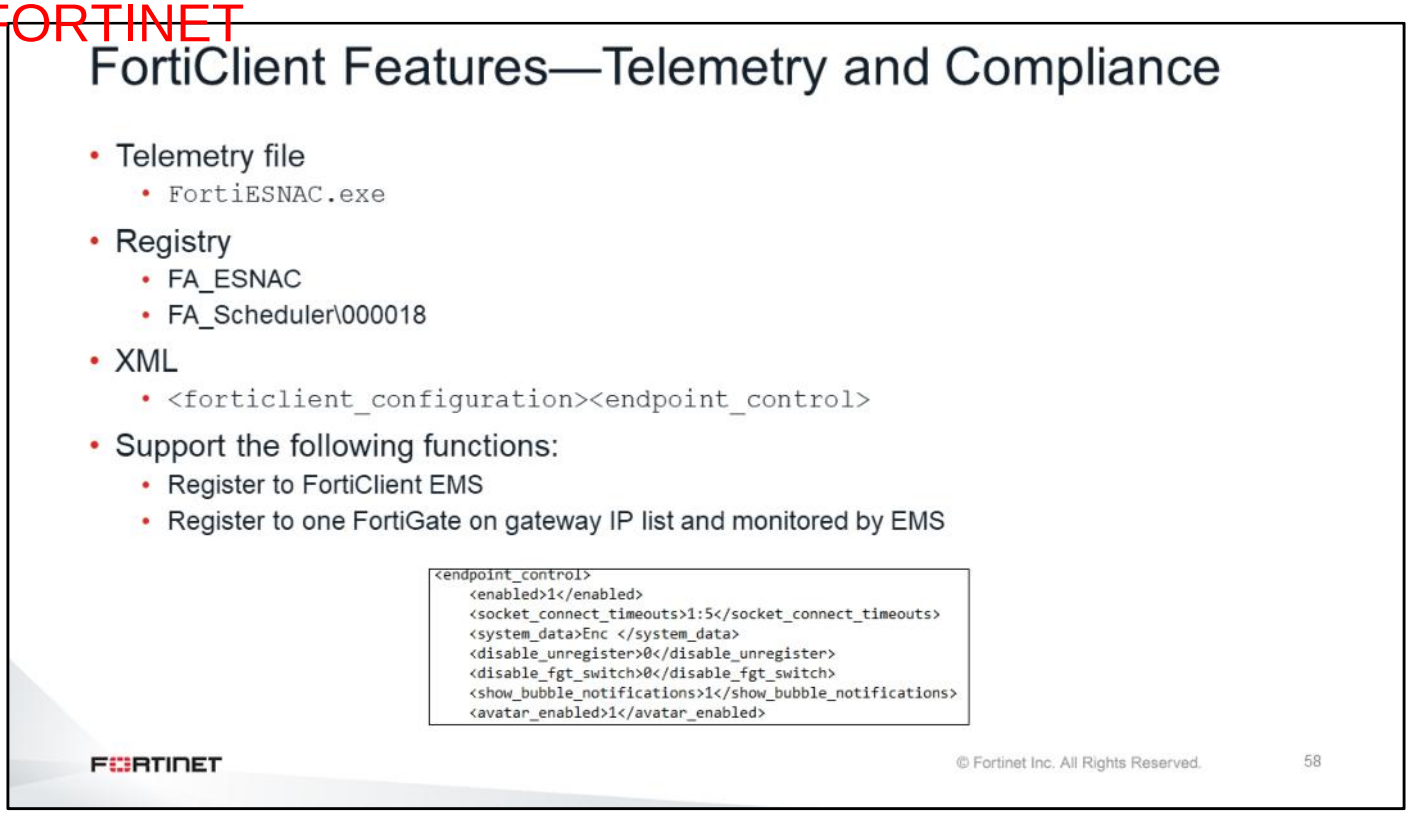
The FortiClient vulnerability scan module can check your workstation for known system vulnerabilities. It uses various files and drivers to perform a vulnerability scan. You can scan your workstation when registering on FortiGate, or on a scheduled basis. Or you can run an on-demand scan directly from the FortiClient GUI and view the vulnerabilities found on the FortiClient console.

You can view the recent vulnerabilities detected directly on the FortiClient GUI, or you can export logs from **Export logs** option.

The vulnerabilities logs shows the status (`started`, `cancelled`) and also shows the name of the vulnerabilities detected, the severity, the vulnerabilities engine, signatures used, and so on. It also provides a reference link, which provides the description, impact, and recommended actions for the vulnerability detected.

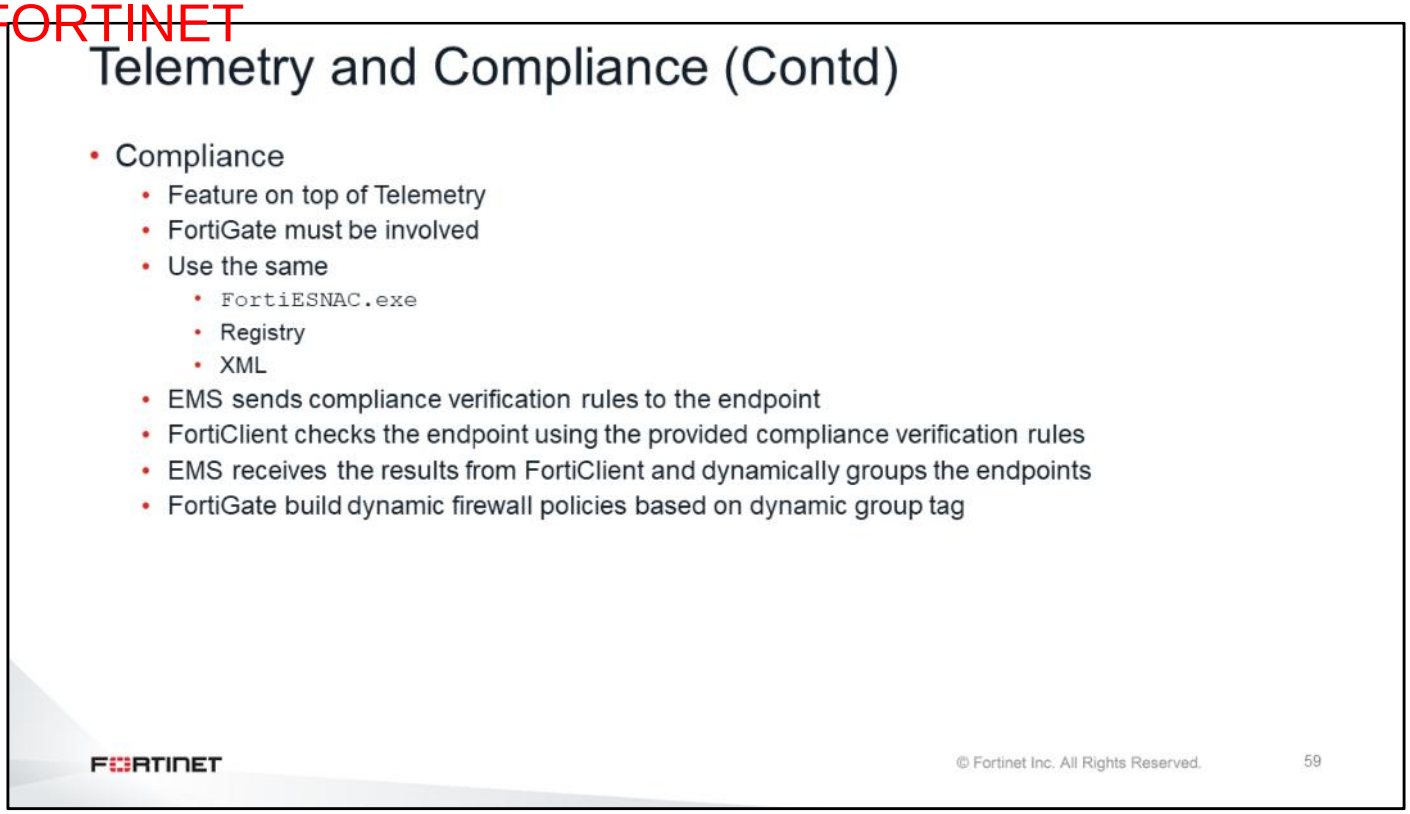


You can run a vulnerability scan in debug mode from the command line in elevated mode. After running the commands shown on this slide, the log file will be available at the following location: `Forticlient_install_folder/logs/vcm/timestamp_folder`



FortiClient requires one file, `FortiESNAC.exe`, for Telemetry. The endpoint-related information is contained inside the `endpoint_control` XML tag. The `endpoint_control` XML tag contains configurations specifically related to endpoint Telemetry.

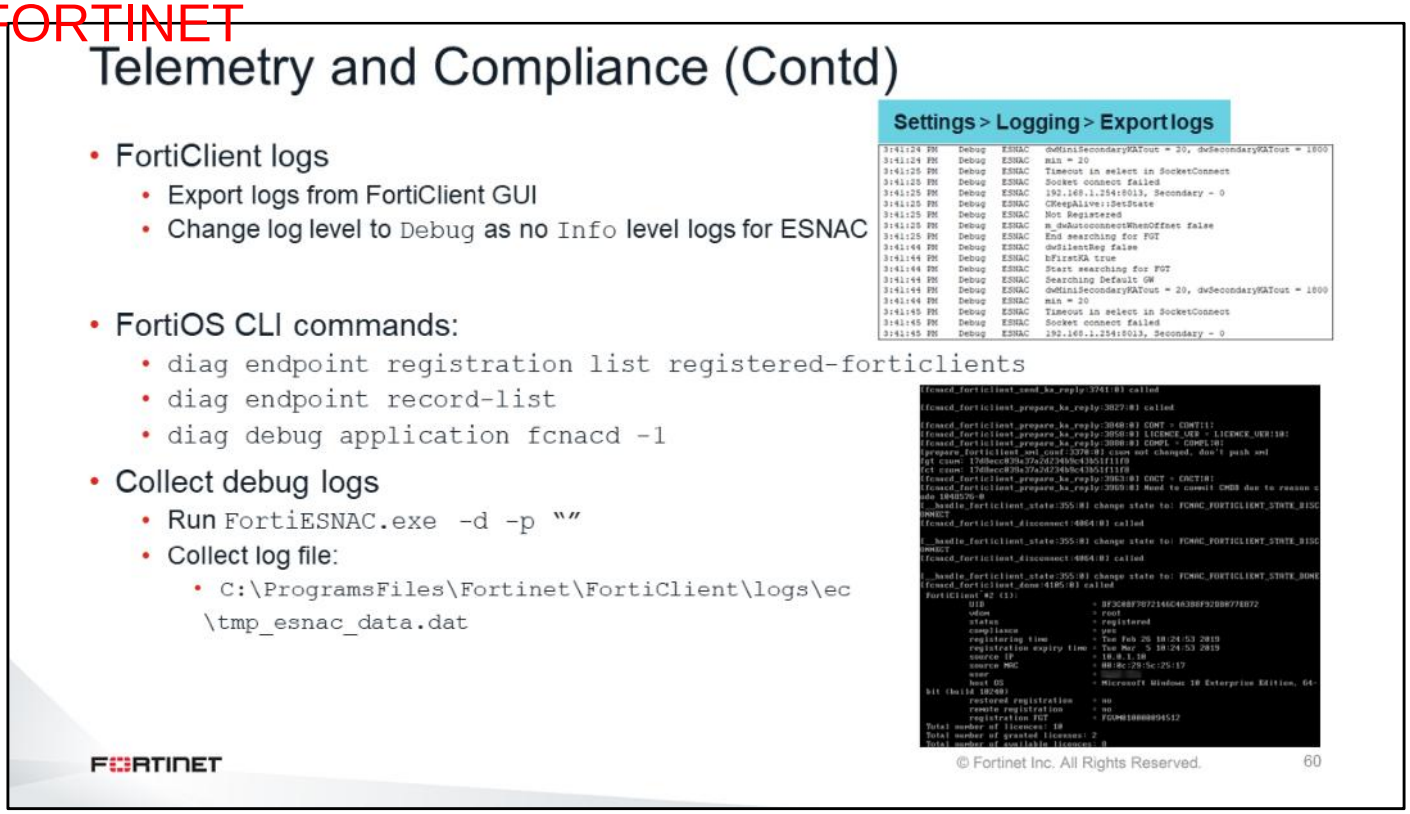
It contains endpoint UI settings, on-net addresses, FortiGate details to register, NAC rules, and user-defined connections.



Compliance is the feature that runs on top of Telemetry. FortiGate must be involved. It uses the same `FortiESNAC.exe`, registry, and XML.

In FortiClient EMS version 6.2.0 or later, FortiClient Telemetry connects to EMS to receive a profile of configuration information as part of an endpoint policy and to FortiGate to participate in the Fortinet Security Fabric. The following summarizes how compliance enforcement occurs:

1. The FortiClient EMS administrator creates compliance verification rules based on the OS, running process and so on.
2. EMS sends compliance verification rules to the endpoint.
3. FortiClient checks the endpoint using the provided compliance verification rules and sends the results to EMS.
4. EMS receives the results from FortiClient and dynamically groups the endpoints according to the results.
5. FortiOS pulls the dynamic endpoint group information from EMS. You can use this tag to build dynamic firewall policies.
6. The FortiGate receives dynamic endpoint group lists from EMS and use them to build dynamic firewall policies to enforce compliance.
7. EMS sends group updates to FortiOS, and FortiOS uses the updates to adjust the policies based on those groups.



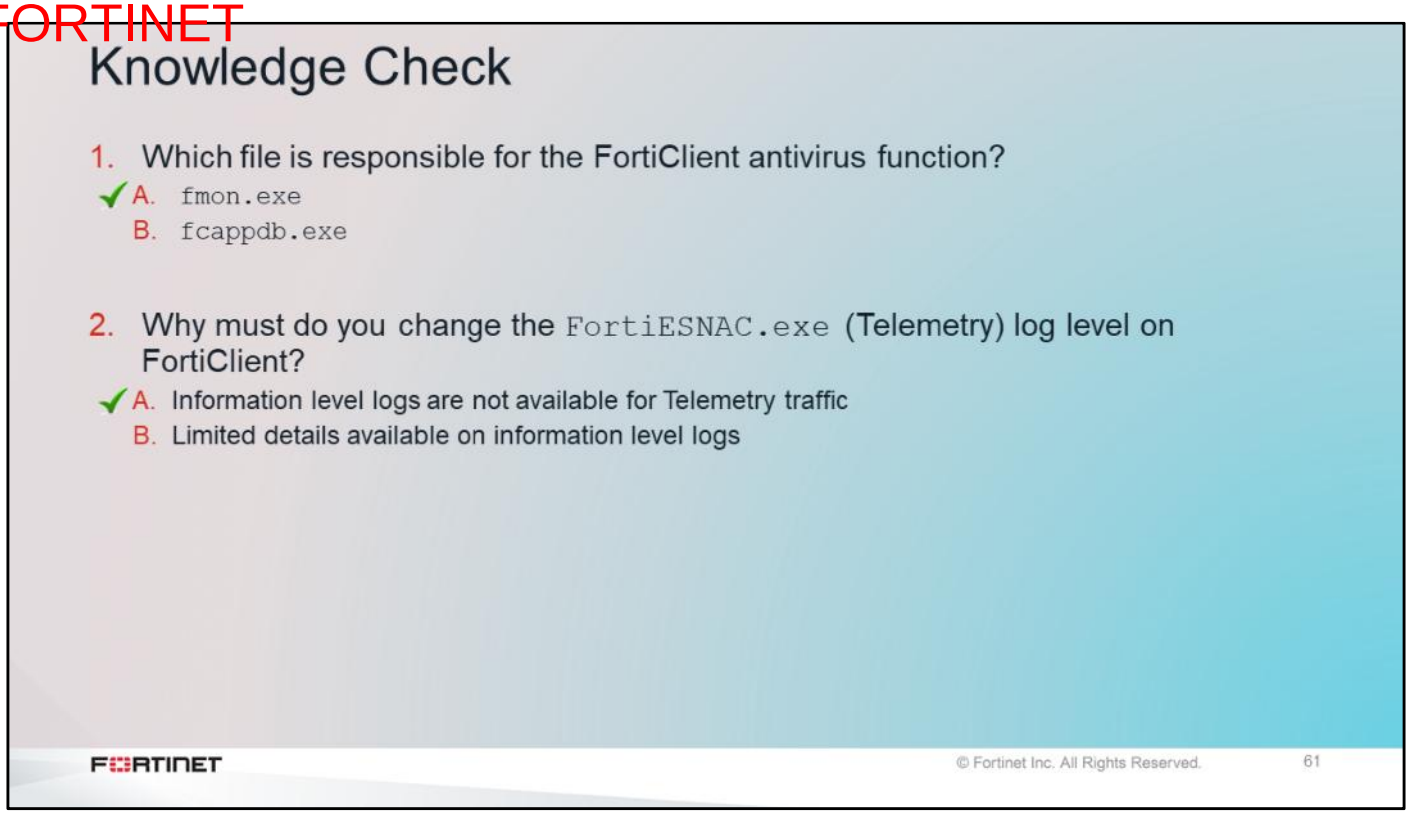
You can export Telemetry and compliance-related logs from **Export logs** option. When troubleshooting these issues, as a best practice, change the log level to `Debug` because there is no `Info` level logs for FortiESNAC process. All Telemetry and compliance-related logs will be tagged with ESNAC.

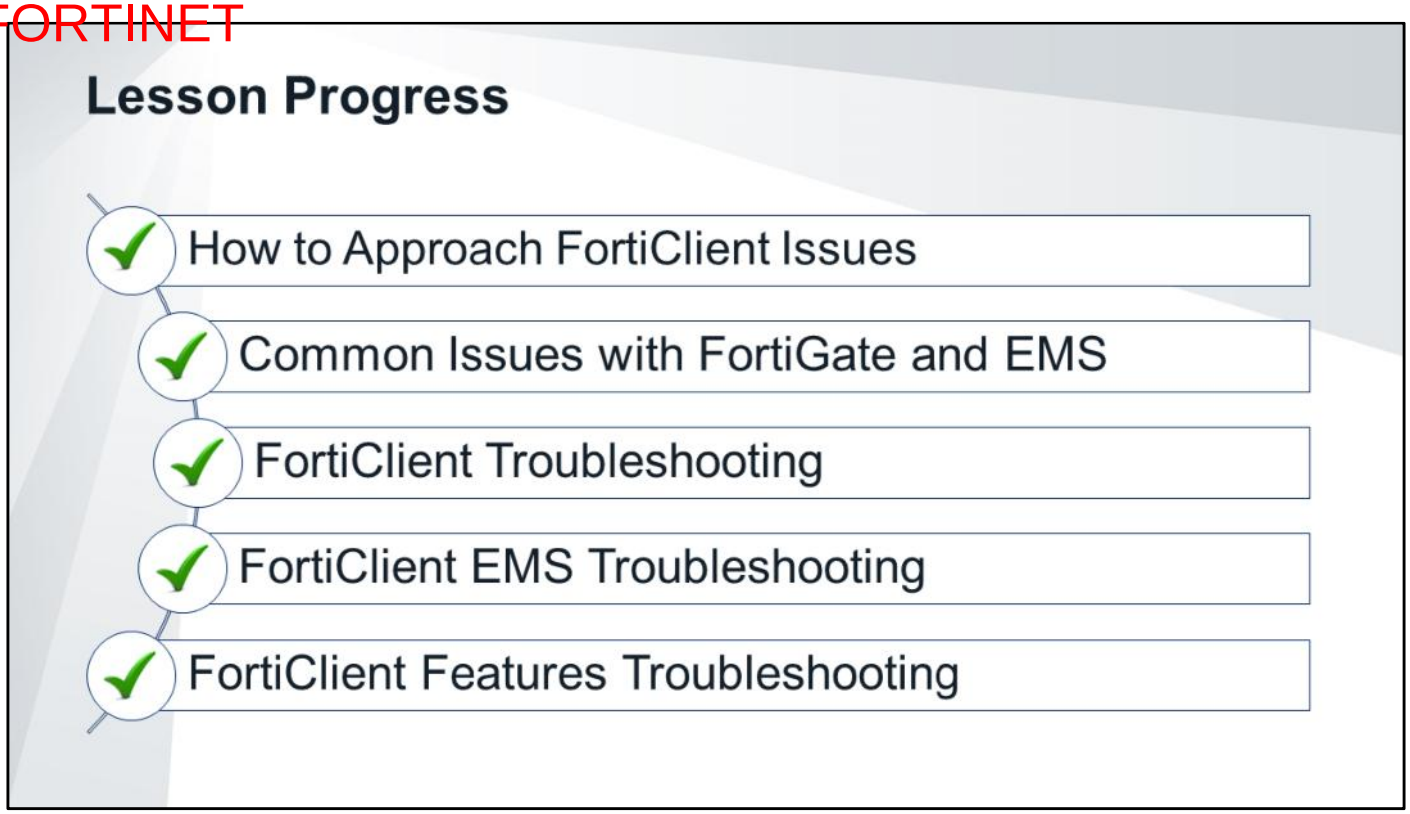
You can collect debug logs on an endpoint using the following steps:

1. Disconnect FortiClient from EMS.
2. Shut down FortiClient.
3. On the administrator command line, run `sc stop fortishield.`
4. Change registry (depends on 32-bit or 64-bit Windows) as shown below:

   `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Fortinet\FortiClient\FA_Scheduler\00 0018\cmd to FortiESNAC.exe -d` (-p <password > is optional).
5. Run FortiClient and register EMS as usual.
6. Collect log file from location shown in this slide.

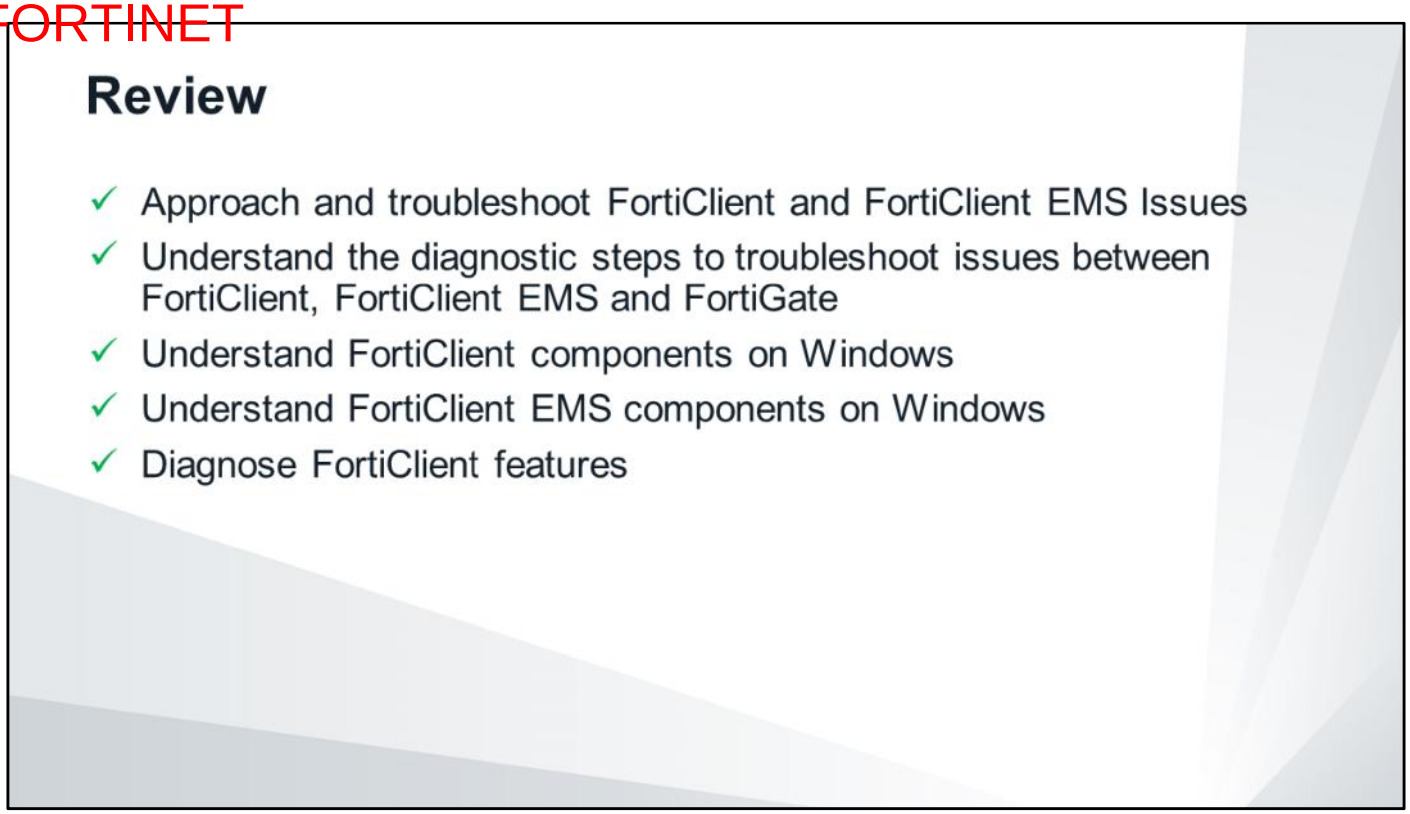
For ESNAC traffic, select file `tmp_esnac_data.dat`.





Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.



This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to approach FortiClient issues and common issues with FortiClient with FortiGate and EMS and, how to diagnose and troubleshoot FortiClient features.